

[0013] FIG. 20 is a diagram showing a content distribution model of the conventional content usage control system. A decrypt protection area and a reproduction protection area of FIG. 20 correspond to the confidential protection area shown in FIG. 18. The decrypt protection area is where the hardware and software are protected against alteration and the output data against duplication, and the reproduction protection area is where the digital decrypted data are protected against duplication. Usage environment specifying physical elements (PCSUE) 235-1 to 235-N are physical elements for specifying the usage environment of the content, and specifically include a CPU, peripheral equipment, a removable storage medium, an IC card and the like.

[0049] A content usage control system, a content usage apparatus and a computer readable recording medium having recorded therein a program for enabling the computer to execute a method of using the content usage apparatus will be explained with reference to the accompanying drawings.

[0050] FIG. 1 is a diagram showing a configuration of a content usage control system according to an embodiment of the invention. A content usage control system 10 shown in FIG. 1 is for controlling the usage by the user 2 of the content of a copyrighted object produced by a copyright holder 1. In FIG. 1, the content usage control system 10 roughly comprises a copyright holder system 20, a content server 30, a license server 40 and a user system 50.

[0051] The copyright holder system 20 includes a confidential content registration section 21 for performing the process of encrypting the content and registering the confidential content in the content server 30 (S10), an access control right delegation section 22 for delegating the access control right by sending to the license server 40 the content decrypt key required for decrypting the encrypted content (confidential content) (S12) and an ACL setting section 23 for setting the usage permit conditions, i.e. the license (ACL) in the license server 40 (S14), thereby managing the usage control of the content of copyrighted objects.

[0052] The content server 30 registers the confidential content sent from the copyright holder system 20 and in response to a confidential content distribution request (S16) from the user system 50, sends out to the user system 50 the registered confidential

content in encrypted form (S17).

[0053] The license server 40 includes a license permission/production section 41 and an LDAP system 42. In response to a content usage request from the user system 50 (S18), the license permission/production section 41 searches the LDAP system 42 for the physical element ID certificate added to the usage request and the corresponding decrypt key, decrypts the physical element ID, searches for the content decrypt key corresponding to the content of which the usage is requested, and sends the license in which the content decrypt key thus searched is encrypted by the physical element ID (S21).

[0100] The internal procedures of the process of the user system 50 will be explained with reference to the flowchart shown in FIG. 11. In FIG. 11, the first step is for the user system 50 to determine whether a request for content usage has been issued or not (step S500). In the case where no request for content usage is issued (NO in step S500), the same determination process is repeated. In the case where a request for content usage is issued (YES in step S500), on the other hand, the content usage request is sent (step S501). After that, it is determined whether a request for a certificate of a physical element has been issued from the license server 40 (step S502), and if there is no request for the certificate of the physical element (NO in step S502), the process proceeds to step S508.

[0101] In the case where the request for a certificate of a physical element is issued (YES in step S502), on the other hand, the physical element ID certificate is read out (step S503), and it is determined whether the read operation has failed or not (step S504). In the case where the read operation is a failure (YES in step S504), an error notice is sent to the license server (step S505), and the process proceeds to step S500. In the case where the read operation is not a failure (NO in step S504), on the other hand, it is determined whether the next physical element is available or not (step S506), and if available (YES in step S506), the process proceeds to step S503 where the next physical element ID certificate is read out and the process described above is repeated.

[0102] In the absence of a next physical element (NO in step S506), on the other hand, a group of the physical element ID certificates are sent to the license server 40 (step S507), and it is further determined whether the received data is an error or a license (step S508). In the case where the received data is an error (ERROR in step S508), the process proceeds to step S500 for repeating the same process as described above, while

in the case where the received data is a license (LICENSE in step S508), the license is further delivered to the physical element (PCSUE) 1 (step S509), followed by proceeding to step S500 to repeat the same process as described above. As a result, the user system 50 can acquire a license from the license server 40.

[0103] The PCSUE 1 is indicative of the first one of (N-1) PCSUEs. A general expression of PCSUE is PCSUE_i where *i* is an integer of 1 to (N-1). The internal procedures of the process performed when the license is delivered to each PCSUE_i will be explained with reference to the flowchart of FIG. 12.

[0104] In FIG. 12, the first step is for the PCSUE_i is to decrypt the received license with K_{pi} (step S600). After that, the decrypted access condition AC_i is evaluated (step S601), and it is determined whether the evaluation result of the access condition AC_i is good or not (step S602). In the case where the evaluation result of the access condition AC_i is not good (NOT GOOD in step S602), the error processing is effected (step S604) to end the process. In the case where the evaluation result of the access condition AC_i is good (GOOD in step S602), on the other hand, the decrypted license is transmitted to the PCSUE (i+1) to continue the decrypting operation, thus terminating the internal processing of the PCSUE_i.

[0105] Then, in PCSUE(i+1), which corresponds to PCSUE(N), the physical element of the reproduction device performs the internal processing, for example. The steps of this internal processing procedure will be explained with reference to the flowchart shown in FIG. 13. In FIG. 13, the first step is to decrypt the received license with K_{pn} (step S700). After that, the decrypted access condition AC(N) is evaluated (step S701), and it is determined whether the result of this evaluation is good or not (step S702). In the case where the result of evaluation is not good (NOT GOOD in step S702), the error processing is performed (step S703) thereby to end the process, resulting in the failure to decrypt the confidential content.

[0106] In the case where the result of evaluation of the access condition AC(N) is good (GOOD in step S702), on the other hand, the confidential content are decrypted with the decrypted K_c (step S704), and the decrypted content are reproduced by the reproduction device (step S705) thereby to end the process.

[0107] A specific license decrypting process will be explained with reference to FIG. 14. In FIG. 14, the license generated by the license server 40 is encrypted by encrypting the access control list ACL and the content decrypt key using the key K_p constituting the physical element ID of the reproduction device 144. The license is further encrypted using, as a key, the value of the exclusive OR of the DSN 141 constituting the serial number of the storage device and the MSN 143 constituting the serial number of the

medium 142.

[0108] First, the storage device 140 reads the write inhibited MSN in the medium 142, and the exclusive OR is calculated between the same value and the DSN of the storage device 140, and according to the calculation result, the license is decrypted into {ACL, Kc}Kp. This partially decrypted license is sent to the reproduction device 144, which in turn decrypts the license using the key Kp constituting the physical element ID of the reproduction device 144 itself, thus acquiring the access condition list ACL and the content decrypt key Kc. In the case where the access condition indicated by the access condition ACL is satisfied, the content decrypt key Kc can be used for decrypting, and the decrypted content are reproduced by the reproduction device 144.

[0109] The process of decrypting the content by requesting and acquiring the license described above will be explained in more detail with reference to the data flow shown in FIG. 15. In FIG. 15, in the decrypt protection area of the user system 50, the license request process 152 is sent to the license server 40 with the physical element ID certificate in order to use the content. In the process, the physical element ID certificate is acquired from the usage environment specifying physical element 150 by the usage environment specifying physical element certificate acquisition process 153 and delivered by the license request process 152.

[0110] Upon transmission of the license from the license server 40, on the other hand, the license acquisition process 156 acquires the license and the access permit process 155 acquires the license from the license acquisition process 156. At the same time, the usage environment specifying physical element ID authentication process 154 acquires the physical element ID through the usage environment specifying physical element certificate acquisition process 153 and further the usage state from the accounting process 157, so that the decrypt key is retrieved using these results.

[0111] The content decrypting process 159 decrypts the confidential content 158 using the content decrypt key and outputs the plain text. The accounting process 157 notifies the usage state monitor physical element 151, whereby the current usage state is automatically decremented in accordance with the usage by the usage environment monitor physical element 151.

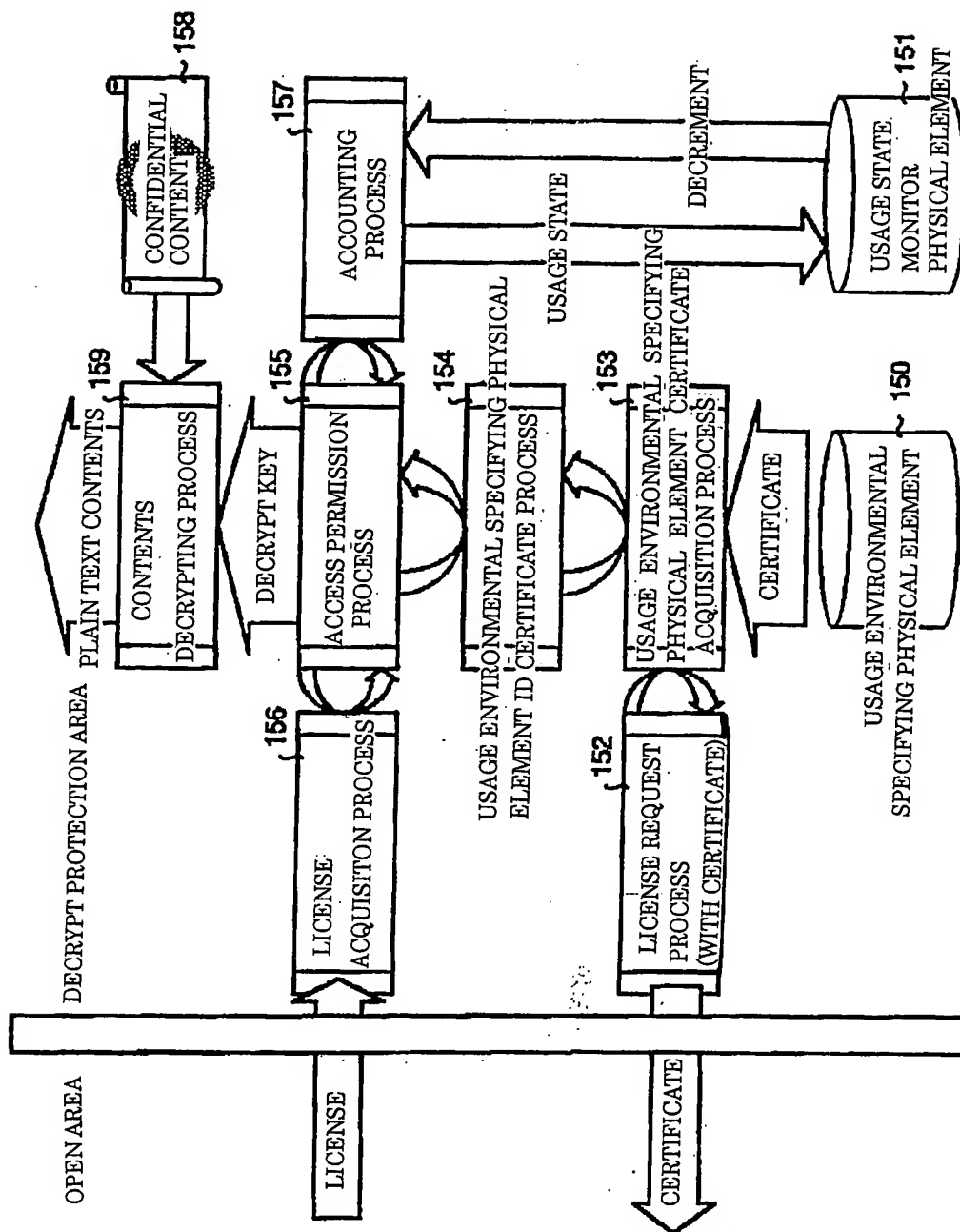


FIG.15

FLOW CHART INDICATING CONTENTS DECRYPTING PROCESS BY REQUESTING AND ACQUIRING LICENSE

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-293439
(P2000-293439A)

(43) 公開日 平成12年10月20日 (2000. 10. 20)

| (51) Int.Cl. ⁷ | 識別記号 | F I | テーマコード* (参考) |
|---------------------------|-------|---------------|-------------------|
| G 0 6 F 12/14 | 3 2 0 | G 0 6 F 12/14 | 3 2 0 B 5 B 0 1 7 |
| 15/00 | 3 3 0 | 15/00 | 3 3 0 D 5 B 0 8 5 |

審査請求 未請求 請求項の数11 O L (全 29 頁)

(21) 出願番号 特願平11-99482

(22) 出願日 平成11年4月6日 (1999. 4. 6)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 畠山 卓久

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(72) 発明者 吉岡 誠

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

(74) 代理人 100089118

弁理士 酒井 宏明

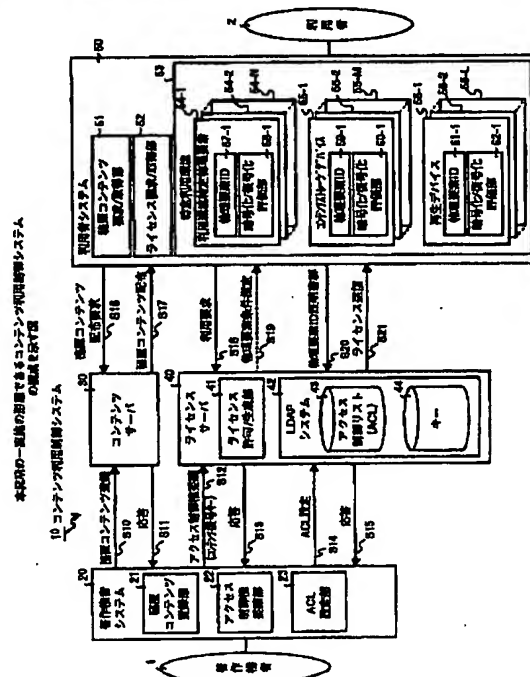
最終頁に続く

(54) 【発明の名称】 コンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができる。

【解決手段】 著作権者システム20とコンテンツサーバ30とライセンスサーバ40と利用者システム50とを有し、著作権者システム20のACL設定部23は、利用者システム50で使用するメディアを含む複数の物理要素のIDおよび利用者IDに基づいてコンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件ACLとして設定し、アクセス制御リスト43に格納する。ライセンスサーバ40は、このアクセス制御リスト43を用いて利用者2によるコンテンツの利用を制御するが、このアクセス制御リストには、コンテンツの利用状況に応じた条件、たとえば操作可能回数最大値や課金条件等の会計条件も設定することができる。



【特許請求の範囲】

【請求項1】 コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、前記コンテンツを利用者が利用する利用者手段と、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定する設定手段と、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御する利用制御手段と、を備えたことを特徴とするコンテンツ利用制御システム。

【請求項2】 前記設定手段が設定する部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件を含むことを特徴とする請求項1に記載のコンテンツ利用制御システム。

【請求項3】 前記利用制御手段は、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成する生成手段を備え、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うことを特徴とする請求項1または2に記載のコンテンツ利用制御システム。

【請求項4】 前記生成手段は、前記利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行うことを特徴とする請求項3に記載のコンテンツ利用制御システム。

【請求項5】 前記物理要素は、他の物理要素に含まれた物理要素を含むことを特徴とする請求項1～4のいずれか一つに記載のコンテンツ利用制御システム。

【請求項6】 開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバをさらに備えたことを特徴とする請求項1～5のいずれか一つに記載のコンテンツ利用制御システム。

【請求項7】 コンテンツの作成者である情報作成者お

よび該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、

コンテンツの利用要求を行い、当該コンテンツ利用要求に応じて送られる許諾要求を当該手段の物理要素の識別情報をもとに復号して得られた利用許可条件を満足する場合に前記コンテンツの復号キーを用いて暗号化されたコンテンツの復号を行う利用者手段と、

前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を予め設定する設定手段と、

前記設定手段によって設定された利用許可条件を格納する条件格納手段と、

前記コンテンツの復号キーを保持する保持手段と、

前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出する抽出手段と、

前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する生成手段と、

を備えたことを特徴とするコンテンツ利用制御システム。

【請求項8】 ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置において、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求手段と、

前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段と、

前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段と、

を備えたことを特徴とするコンテンツ利用装置。

【請求項9】 ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、

コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求工程と、

前記コンテンツの利用要求に対応してコンテンツ管理装

置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程と、

前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段と、

を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項10】 利用者がコンテンツの利用を行うコンテンツ利用装置において、

前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段と、

前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う手段と、

を備えたことを特徴とするコンテンツ利用装置。

【請求項11】 利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、

前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程と、

前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う工程と、

を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、著作権者等の情報提供権限者が開放ネットワークを介して提供するコンテンツの利用を制御するコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【0002】 貨幣の役割は、その貨幣という物質としての性質によって、公平な報酬を人々に提供する。貨幣というオブジェクトは、単なる口約束的共有概念ではなく、物理的に存在し、携帯でき、さらに発行元以外による偽造が困難であることが必須要件であった。物理的に存在し、携帯できることによって、その価値の利用者同士で公平に確認することができ、偽造の困難性によって、その公平な確認の契機を公平なる貨幣の発行元がコントロールすることができた。しかし、近年の工業技術の発展によって、今や貨幣の偽造困難性が崩壊する日が

近い。貨幣に代わる新たな価値確認オブジェクトが必要になっている。そのオブジェクトはやはり、まず物理的に存在し、携帯でき、偽造困難である必要がある。さらにそのオブジェクトは発行元がアクセスコントロールできる必要がある。

【0003】 このセキュリティ強化面からの要求に加え、情報流通の多様化と大容量化、高速化の側面から「超流通」の実現の要求も高まっている。この「超流通」を実現した環境は、つぎの条件を満足する。すなわち、(1) 情報利用者は、デジタル情報をほぼ無料で入手できること、(2) 情報提供者は、その情報の利用を許可する条件(課金、改変利用条件など)を指定し、利用者の合意した条件を強制することができること、

(3) このサービスを利用するに当たって、必要な情報利用者の追加操作は「アクセス条件の確認」程度であること、である。

【0004】 こうした超流通のアクセス制御を正確かつ、安全に実行可能なシステムは、ライセンス料などの著作権料徴収の不公平の是正にも寄与することが期待できる。現行システムでは、著作物が相当数売れないと提供者は利益を上げられないが、正確に著作権者の手に渡るようにシステムを構築できることが望まれる。また、専門家的芸術家から、部品としての創作を提供するデザイナーに至るまで、各人のサービス料に見合う報酬が公平に分配されることが望まれる。

【0005】

【従来の技術】 従来、著作物等のコンテンツに対するアクセスを分散システム環境、特に開放ネットワーク上において制御する場合、コンテンツの利用者からのアクセスが可能なサーバにコンテンツを格納し、このサーバに対するアクセスを制御することによって、コンテンツの利用を制御していた。ここで、コンテンツとは、単一の記憶装置媒体に記録可能なビット列の集合としての構造をもつデジタルコンテンツであり、文書テキスト、画像、動画、プログラムソフトウェア等を含む。

【0006】 たとえば、図17は、従来のアクセス制御モデルを示す図である。図17において、コンテンツ204は、アクセス制御機能203を介してのみ、利用者205からのコンテンツ操作を可能としている。また、著作権者200は、コンテンツ204をアクセス制御機能203で保護された、たとえばサーバに登録するのみで、著作権者200以外の者、たとえばこのサーバを管理する管理者によってアクセス制御機能203に対するアクセス制御操作がなされていた。

【0007】 すなわち、図18に示すようにコンテンツを保持するサーバシステム212は、管理者201によって管理運用されるサーバ運用者システム211によって管理され、サーバ運用者システム211は、サーバシステム212に対して著作権者および利用者登録を行い、またこのためのディレクトリ生成を行い、さらに

は、著作権者によるアクセス制御を許可することも行う。著作権者システム 210 は、著作権者の著作物のコンテンツをサーバシステム 212 に保存させ、アクセス制御条件 (ACL) をサーバシステム 212 に対して設定する。この場合、著作権者は、サーバシステム 212 に対してアクセス制御の許可を得なければならない。一方、利用者システム 213 は、コンテンツの利用に際して、コンテンツ送信要求をサーバシステム 212 に対して行い、ACL を満足する場合には、サーバシステム 212 内に保存されていたコンテンツを取得する。

【0008】しかし、コンテンツの利用者にすべての権限が与えられ、移動やコピー (複製) によって利用者が変わると、移動あるいはコピー先のコンテンツに対しては、もとの著作権者の権限はまったく働かない。また、コンテンツオブジェクトを保存するサーバ管理者と著作権者の間では、オブジェクトに対するアクセス許諾強制のあり方も明確ではなく、たとえばサーバ管理者が著作権者に断りなく、アクセス権を変更可能なことが当然のこととされていた。

【0009】一方、近年の記憶媒体等の低価格化等によって分散システム環境が促進され、ネットワークのトラフィックが集中することなく、コンテンツを複数のサーバにキャッシュして分散できるようになり、コンテンツオブジェクトに対するアクセスを高速に行うことができるようになった。従って、図 17 に示すようなアクセス制御モデルは、利用者 205 によるコンテンツ操作への入り口のみに対して強固なアクセス制御機能を構築すればよいが、上述した分散システム環境下では、全方向的なアクセス制御あるいはセキュリティ保護を行う必要があった。

【0010】そこで、図 19 に示すようなアクセス制御モデルが考えられた。このアクセス制御モデルでは、著作権者 200 が従来のセキュリティ技術で保護が可能な領域である著作権者保護領域と、あらゆる外部からの攻撃を受容する開放領域と、ハード/ソフトの改ざんの保護とデジタルデータ複製防止処理が施される秘匿保護領域とに分離される。秘匿保護領域は、全方向的なアクセス制御機能 221 によって保護し、このアクセス制御機能 221 内にコンテンツ 222 が保存される。

【0011】このコンテンツに対して、著作権者 200 は、コンテンツ 222 の登録とともに、アクセス制御機能 221 に対するアクセス制御操作も可能としている。利用者 205 は、開放領域から、アクセス制御機能 221 を介してコンテンツ 222 を取得することになる。なお、領域間保護インターフェース 220 は、著作権者保護領域と開放領域との間の保護を行うインターフェースである。

【0012】この図 19 に示す分散システム環境下におけるアクセス制御モデルの具体化は、米国特許 5339433 号公報に記載されており、また、特開平 9-13

4311 号公報、米国特許 5392351 号公報、米国特許 555304 号公報、および米国特許 5796824 号公報には、利用者の機器をチェックしてコンテンツの不正利用を防止する技術が記載されている。以下、これらの公報を参照して従来のコンテンツ利用制御システムについて説明する。

【0013】図 20 は、従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。図 20 において、復号保護領域と再生保護領域とは、図 18 に示す秘匿保護領域に相当し、復号保護領域は、ハード/ソフトの改ざんの保護と出力データの複製防止保護の領域であり、再生保護領域は、デジタル復号データの複製防止の領域である。利用環境特定物理要素 (PCSUE) 235-1~235-N は、コンテンツの利用環境を特定する物理要素であり、具体的には、CPU、周辺装置、リムーバブルな記憶媒体、IC カード等である。

【0014】復号保護領域では、PCSUE 235-1~235-N に対応する物理要素 ID の証明書 236-1~236-N をもとに、著作権者 200 によって暗号化されたコンテンツ 233 の複製であって開放領域のサーバに存在するコンテンツ 234 を復号し、再生保護領域を介して、この複合されたコンテンツが利用者に利用される。従って、コンテンツは、物理要素 ID に対応したキーで暗号化され (コンテンツ 233)、このコンテンツ 233 に対応するコンテンツ 234 を復号するためには、各物理要素 ID またはそれに対応した秘密のキーが必要となる。

【0015】ここで、コンテンツ配布モデルには、暗号化されたコンテンツを復号するために用いられるライセンスを、暗号化されたコンテンツと同時に配布するライセンス同時モデルと、暗号化されたコンテンツをサーバのキャッシュに保存し、ライセンスとは別のタイミングで取得するコンテンツキャッシュ可能型モデルとがある。図 21 は、このコンテンツキャッシュ可能型モデルを示す図である。

【0016】図 21 において、まず著作権者 200 は、著作権者保護領域で、コンテンツを生成し、このコンテンツを暗号化し、その後、複製して開放領域のサーバ等にキャッシュされる。一方、PCSUE 235-1~235-N の物理要素 ID を暗号化した証明書 241-1~241-N は、暗号化された状態で著作権者保護領域に出力され、PCSUE 235-1~235-N に対応する利用者物理オブジェクトクラスから秘密キー Kp を取り出し、この秘密キー Kp と証明書 241-1~241-N とから物理要素 ID 243-1~243-N を復号し、この物理要素 ID 243-1~243-N によってコンテンツ復号キー Kc を暗号化し、秘密保護領域に出力する。

【0017】秘密保護領域では、暗号化されたコンテンツ復号キー Kc を物理要素 ID 242-1~242-N

で復号し、コンテンツ復号キーKcを得る。このコンテンツ復号キーKcを用いて開放領域から取得される、暗号化されたコンテンツ234を復号し、コンテンツ244として利用者205に利用させる。

【0018】図22は、図21に示すコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示すブロック図である。図22において、著作権者システム250は、著作権者保護領域に存在し、コンテンツサーバ251は、開放領域に存在し、ライセンスサーバ252および利用者システム253は、秘匿保護領域に存在する。著作権者システム250は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ251に保存しておく。

【0019】また、コンテンツ復号キーKcをライセンスサーバ252に送信して、アクセス制御権の委譲をライセンスサーバ252に対して行う。さらに、アクセス制御リスト(ACL)設定を行う。利用者システム253は、コンテンツを利用することを示す利用要求をライセンスサーバ252に送信し、このとき、物理要素IDの証明群が添付されていない場合には、ライセンスサーバ252の物理要素条件指定によって物理要素IDの証明群を取得し、ライセンスサーバ252に送出する。

【0020】ライセンスサーバ252は、図21に示したように、利用者の物理オブジェクトクラスの秘密キーKpを取得して物理要素ID証明群を復号し、復号した物理要素IDによって暗号化されたコンテンツ復号キーKcがライセンスLとして利用者システム253に送出される。これによって、利用者システム253の物理要素IDが一致すれば、復号が行われ、この復号されたコンテンツ復号キーKcを用いて秘匿コンテンツを復号することができる。

【0021】なお、秘密コンテンツはコンテンツサーバ251に保存されているので、利用者システム253は、別途コンテンツサーバ251に秘密コンテンツ配布要求を行って、コンテンツサーバ251から秘密コンテンツの配布を受ける必要がある。

【0022】一方、図23は、コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成ブロック図を示している。図23では、コンテンツサーバ251が存在せず、ライセンス送信と同時に利用者システム253に送付されることになる。図22に示すように、コンテンツサーバ251を介して秘密コンテンツを取得する場合、秘密コンテンツは予め時間的に利用者システム253に近いサーバまで運ばれているので、利用者システム253は、コンテンツが必要な時に利用要求をすればよい。

【0023】また、コンテンツ同時配布型モデルに比較してコンテンツの流通経路の適切な選択が可能となり、利用者にとっては、コンテンツ取得に際して応答時間の

短縮が期待できる。また、コンテンツキャッシュ可能型モデルでは、コンテンツを、ライセンスの提供とは別に、ROM媒体ベース、放送、Proxyサーバによるキャッシュ等によって、予め配布しておくことが可能であり、利点が多い。

【0024】

【発明が解決しようとする課題】しかしながら、上述した従来のコンテンツ利用制御システムでは、利用者システムに固有の物理要素IDに一致する装置であれば、基本的に秘匿コンテンツを復号でき、このコンテンツを利用することができるが、この物理要素IDのみによってライセンス(利用許可条件)を生成しているのので、たとえば、著作権者の意思で決定されるコンテンツの読み出し回数を制限する条件を付加したり、時間制限を設けたり、課金条件を設定したりすることができず、柔軟なコンテンツ利用制御ができないという問題点があった。

【0025】また、利用環境特定物理要素は、常に単純な構成となつてとは限らず、複雑な構成をもった機器である場合には、その機器のうちの特定の機器あるいは部品が不正である場合もあり、このような場合に、単に大きな構成の機器である利用環境特定物理要素によって利用許可条件を生成しても、不正を見逃してしまうこととなりセキュリティが低下するという問題点があった。

【0026】この発明は上記に鑑みてなされたもので、著作権者等の情報作成者に許諾された者を含む情報提供権限者がコンテンツ利用制御を柔軟に行うことができるとともに、コンテンツの不正利用を精度高く防止することができるコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0027】

【課題を解決するための手段】上記目的を達成するため、請求項1にかかる発明は、コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、前記コンテンツを利用者が利用する利用者手段(図1の50)と、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定する設定手段(図1の23)と、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御する利用制御手段(図1の40)と、を備えたことを特徴とする。

【0028】この請求項1にかかる発明によれば、設定手段が、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利

用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定し、前記利用制御手段は、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御し、利用許可条件に基づいた柔軟な利用制御を可能とする。

【0029】また、請求項2にかかる発明は、請求項1に記載のコンテンツ利用制御システムにおいて、前記設定手段が設定する部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件（図3の会計条件値に相当）を含むことを特徴とする。

【0030】この請求項2にかかる発明によれば、設定手段によって設定される部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化するカテゴリーに対する条件である会計条件を含むようにし、一層利用者に対する利用制御を細かに行うことができる。

【0031】また、請求項3にかかる発明は、請求項1または2に記載のコンテンツ利用制御システムにおいて、前記利用制御手段（図1の40）は、前記利用者手段（図1の50）からのコンテンツ利用要求（図1のS18）を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成する生成手段（図1の41）を備え、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うことを特徴とする。

【0032】この請求項3にかかる発明によれば、生成手段が、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成し、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行う。

【0033】また、請求項4にかかる発明は、請求項3のコンテンツ利用制御システムにおいて、前記生成手段（図1の41）は、前記利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して（数1および数2に相当）行うことを特徴とする。

【0034】この請求項4にかかる発明によれば、利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行い、一部の物理要素に対する攻撃成功によるコンテンツ復号キーの盗難の危険性を分散することができる。

【0035】また、請求項5にかかる発明は、請求項1～4に記載のコンテンツ利用制御システムにおいて、前記物理要素は、他の物理要素に包含された物理要素（図9の131～136）を含むことを特徴とする。

【0036】この請求項5にかかる発明によれば、物理要素が包含関係にある物理要素であっても一つの物理要素として取り扱い、この一つの物理要素の不正も許さず、コンテンツ復号キーの盗難という危険性を分散することができる。

【0037】また、請求項6にかかる発明は、請求項1～5に記載のコンテンツ利用制御システムにおいて、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバ（図1の30）をさらに備えたことを特徴とする。

【0038】この請求項6にかかる発明によれば、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバを有しているので、開放ネットワークを十分に活用して当該システムにおけるトラフィックの輻輳を防止して、迅速にコンテンツを獲得することができる。

【0039】また、請求項7にかかる発明は、コンテンツの作成者である情報作成者および該情報作成者によって許諾された者を含む情報提供権限者によって提供される該コンテンツの利用制御を行うコンテンツ利用制御システムにおいて、コンテンツの利用要求を行い、当該コンテンツ利用要求に応じて送られる許諾要求を当該手段の物理要素の識別情報をもとに復号して得られた利用許可条件を満足する場合に前記コンテンツの復号キーを用いて暗号化されたコンテンツの復号を行う利用者手段

（図1の50）と、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を予め設定する設定手段（図1の23）と、前記設定手段によって設定された利用許可条件を格納する条件格納手段（図1の43）と、前記コンテンツの復号キーを保持する保持手段（図1の44）と、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復

号キーを抽出する抽出手段（図 4 2）と、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する生成手段（図 1 の 4 1）と、を備えたことを特徴とする。

【0040】この請求項 7 にかかる発明によれば、設定手段が、利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を前記利用制御手段内の条件格納手段に格納することによって予め設定するとともに、保持手段に前記コンテンツの復号キーを保持する。抽出手段は、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出し、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手段に送出する。利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行う。

【0041】また、請求項 8 にかかる発明は、ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置において、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求手段（図 1 の 5 2）と、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段（図 1 の 5 8-1、60-1、62-1）と、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う手段（図 1 の 5 1）と、を備えたことを特徴とする。

【0042】この請求項 8 にかかる発明によれば、要求手段が、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信すると、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くしている。

【0043】また、請求項 9 にかかる発明は、ネットワークに接続して利用者がコンテンツの利用を行うコンテンツ利用装置のコンピュータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信する要求工程（図 11 の S501）と、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程（図 12 の S600、S601、図 13 の S700、S701）と、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行う工程（図 13 の S704）と、を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0044】この請求項 9 にかかる発明によれば、まず要求工程によって、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信し、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【0045】また、請求項 10 にかかる発明は、利用者がコンテンツの利用を行うコンテンツ利用装置において、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める手段（図 1 の 5 8-1、60-1、62-1）と、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う手段（図 1 の 5 1）と、を備えたことを特徴とする。

【0046】この請求項 10 にかかる発明によれば、まず、コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【0047】また、請求項 11 にかかる発明は、利用者がコンテンツの利用を行うコンテンツ利用装置のコンピ

ユータで実行させるプログラムを格納したコンピュータ読み取り可能な記録媒体であって、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求める工程（図12のS600、S601、図13のS700、S701）と、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行う工程（図13のS704）と、を動作させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【0048】この請求項11にかかる発明によれば、まず、前記コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにして、保護強度を高くする。

【0049】

【発明の実施の形態】以下に添付図面を参照して、本発明にかかるコンテンツ利用制御システム、コンテンツ利用装置およびその利用方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を説明する。

【0050】図1は、本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。図1に示すコンテンツ利用制御システム10は、著作権者1が作成した著作物のコンテンツを利用者2が利用する場合に、この利用を制御するシステムである。図1において、このコンテンツ利用制御システム10は、大きく、著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、および利用者システム50を有する。

【0051】著作権者システム20は、作成したコンテンツを暗号化し、この暗号化した秘匿コンテンツをコンテンツサーバ30に登録する（S10）処理を行う秘匿コンテンツ登録部21、暗号化したコンテンツ（秘匿コンテンツ）を復号するのに必要なコンテンツ復号キーをライセンスサーバ40に送出することによって、アクセス制御権をライセンスサーバに委譲する（S12）処理を行うアクセス制御権委譲部22、および利用許可条件（ACL）をライセンスサーバ40に設定する（S14）ACL設定部23を有し、著作物のコンテンツに関する利用制御を管理する。

【0052】コンテンツサーバ30は、著作権者システム20から送られた秘匿コンテンツを登録し、利用者システム50からの秘匿コンテンツ配布要求があった（S16）場合に、この登録され、保存されている秘匿コンテンツを暗号化された状態で利用者システム50に送出する（S17）。

【0053】ライセンスサーバ40は、ライセンス許可／生成部41とLDAPシステム42とを有する。ライセンス許可／生成部41は、利用者システム50からコンテンツの利用要求があった（S18）場合、この利用要求に付加された物理要素ID証明書とこれに対応する復号キーをLDAPシステム42から検索し、物理要素IDを復号し、利用要求されたコンテンツに対応するコンテンツ復号キーを検索し、この検索したコンテンツ復号キーを物理要素IDで暗号化したライセンスを送信する（S21）。

【0054】このライセンスは、物理環境特定要素条件であり、物理要素の構造に対応させ、論理和と論理積を用いて構造化した組み合わせの形態となっている。また、この実施の形態では、従来から用いられていた物理環境特定要素条件のみならず、利用者の利用状況を条件とした会計条件も併せてACLとして暗号化される。このライセンスの暗号化と復号化については後述する。なお、利用要求（S18）に物理要素ID証明書が付加されていない場合、LDAPシステム42内にも存在しない場合には、物理要素条件指定（S19）を利用者システム50に送付して、利用者システム50が生成した物理要素ID証明書群を返す（S20）。

【0055】一方、著作権者システム20からアクセス制御権委譲によるコンテンツ復号キーが送られてきた（S12）場合は、このコンテンツ復号キーを後述するLDAPシステム42内のキー44のデータベースに秘匿コンテンツに対応させて登録する。また、著作権者システム20からACL設定が送られてきた（S14）には、このACLを秘匿コンテンツに対応させて、LDAPシステム42内のアクセス制御リスト（ACL）に格納する。

【0056】利用者システム50は、秘匿コンテンツの配布要求（S16）と配布された秘匿コンテンツの取得を行う秘匿コンテンツ要求／取得部51と、ライセンスの要求、すなわち利用要求（S18）とライセンスの取得（S21）の処理を行うライセンス要求／取得部52と、利用者システムの特定利用環境（SUE）53とを有する。特定利用環境53とは、特定のコンテンツ利用環境をいい、CPU、周辺装置、リムーバブルな記憶媒体、ICカード、コンテンツ利用状況などの総合的情報をいう。

【0057】特定利用環境には、CPU等の利用環境特定物理要素（PCSUE）54-1～54-Nと、コンテンツを格納するコンテンツストレージデバイス55-1～55-Mと、プレーヤやビューワ等の再生デバイス56-1～56-Lとを有する。各PCSUE54-1～54-N、各コンテンツストレージデバイス55-1～55-M、および各再生デバイス56-1～56-Lは、それぞれの物理要素ID57-1～57-N、59-1～59-M、61-1～61-Lを有するとともに

に、暗号化／復号化／評価部58-1～58-N、60-1～60-M、62-1～62-Lを有する。

【0058】暗号化／復号化／評価部58-1～58-N、60-1～60-M、62-1～62-Lは、各物理要素を暗号化する場合には、自物理要素の物理要素IDで暗号化して出力し、各物理要素の復号化を行う場合には、自物理要素の物理要素IDで復号化を行い、さらに復号結果を評価する処理を行う。すなわち、各物理要素IDの処理に関しては各物理要素毎に行い、物理要素間のインターフェース上であっても、情報が漏れないようにしている。

【0059】つぎに上述した著作権者システム20、コンテンツサーバ30、ライセンスサーバ40、利用者システムの動作処理を主としてフローチャートを参照して説明する。まず、図2のフローチャートを参照して、著作権者システム20の内部処理手順について説明する。

【0060】図2において、著作権者システム20は、まず操作イベントが発生したか否かを判断する(ステップS100)。操作イベントが発生していない場合(ステップS100、なし)には、操作イベントが発生するまでこの処理を繰り返し、操作イベントが発生した(ステップS100、あり)には、操作イベントの操作内容が秘匿コンテンツ登録か、ACL登録か、アクセス制御権委譲かを判断する(ステップS101)。

【0061】操作内容が秘匿コンテンツ登録である場合(ステップS101、秘匿コンテンツ登録)には、秘匿コンテンツ登録部21は、コンテンツの暗号化を行い(ステップS110)、コンテンツサーバリストから所望のコンテンツサーバ30を指定し(ステップS111)、この指定したコンテンツサーバ30に対して秘匿コンテンツ登録要求を行う(ステップS112)。その後、コンテンツサーバ30からの応答を得て、その応答がOKであるかエラーであるかを判断する(ステップS113)。

【0062】コンテンツサーバ30からの応答がOKの場合にはそのまま、エラーである場合には、エラー処理を行った(ステップS114)後、さらに、つぎのコンテンツサーバが指定されたか否かを判断する(ステップS115)。つぎのコンテンツサーバが指定された場合(ステップS115、あり)には、ステップS112に移行して上述した処理を繰り返し、つぎのコンテンツサーバが指定されていない場合(ステップS115、なし)には、ステップS100に移行して上述した処理を繰り返す。

【0063】操作内容がACL設定である場合(ステップS101、ACL設定)、ACL設定部23は、さらに、指定されたコンテンツ復号キーを登録するか否かを判断し(ステップS120)、コンテンツ復号キーの登録をしない場合(ステップS120、なし)には、エラー処理を行って(ステップS124)、ステップS10

0に移行し、上述した処理を繰り返す。一方、コンテンツ復号キーの登録がある場合(ステップS120、あり)には、ACL設定要求をライセンスサーバ40に送信し(ステップS122)、ライセンスサーバ40からACL登録結果を受信し(ステップS123)、その後ステップS100に移行して上述した処理を繰り返す。

【0064】また、操作内容がアクセス制御権委譲である場合(ステップS101、アクセス制御権委譲)には、暗号化したコンテンツ復号キーをライセンスサーバ40に送信し(ステップS130)、暗号化コンテンツ復号キーの登録結果を受信し(ステップS131)、ステップS100に移行し、上述した処理を繰り返す。

【0065】つぎに、ここで、ACL設定部23によって設定されるACLについて説明する。図3は、アクセス条件の一例を示す図であり、アクセス条件は、会計条件と物理環境特定要素(PCSUE)条件との2種類がある。図3に示すように、本発明の特徴の一つである会計条件としては、まず、maxCount(操作可能回数最大値)があり、これに対応するコンテンツの利用状況はcount(操作済回数)である。操作済回数という可変値に対して操作可能回数最大値という制限を設けてアクセスを制御、すなわち限定と認可を行おうとするものである。

【0066】つぎのmaxLength(読み出し最大長さ)の会計条件値に対応するコンテンツの利用状況は、totalLen(読み出し済長さ+被請求読み出し長さ)であり、コンテンツの読み出し最大長さによってアクセスの制御をしようとするものである。つぎのmaxTimeLen(実行可能最大時間)の会計条件値に対応するコンテンツの利用状況は、totalTime(実行済時間長)であり、コンテンツの実行可能最大時間によってアクセスの制御をしようとするものである。つぎのmaxDebt(借入可能金額(課金条件))の会計条件値に対応するコンテンツの利用状況は、debt(残金)であり、残金のマイナス値は借入金額となり、課金条件によってアクセスの制御をしようとするものである。

【0067】また、物理環境特定要素条件としては、まず計算機本体があり、これに対応する物理要素IDのクラスは、PSNであり、プロセッサのシリアル番号である。ここで、クラスとはデータベース上のオブジェクトクラスである。つぎの周辺デバイスに対応する物理要素IDのクラスは、DSNであり、デバイスの種類とシリアル番号を示す。つぎのメディアに対応する物理要素IDのクラスは、MSNであり、メディアの種類とシリアル番号を示す。つぎのICカードに対応する物理要素IDは、certificatesであり、ICカードが発行する証明書を示す。

【0068】つぎの人体部位は、たとえば指紋や網膜(アイリス)情報であり、これに対応する物理要素IDのクラスは、bodyPartsであり、人体部位の認証情報で

ある。つぎの許可する時間帯に対応する物理要素IDのクラスは、timePeriodであり、ローカルクロックやグローバルなGPS時刻である。つぎのネットワークドメインは、ネットワーク上のエリアを示し、これに対応する物理要素IDのクラスは、MACAddressであり、MACアドレスを示す。つぎの地理的位置は、利用国などを示し、これに対応する物理要素IDのクラスは、locationであり、GPSあるいはPHSが検出する位置を示す。つぎの人の記憶に対応する物理要素IDのクラスは、user-ID WithPwdであり、ユーザIDとパスワードを示す。最後のグループに対応する物理要素IDのクラスは、groupであり、物理要素IDの集合を示す。

【0069】このようなアクセス条件は、ANDとORとの論理的な組み合わせをもったセット、すなわちACLとして設定される。アクセス条件には、上述したように会計条件と物理環境特定要素条件とがあるが、これらは任意に組み合わせ可能である。たとえば、一つのACLとしては、つぎのようなものが設定される。すなわち、

```
udac#acl
read: ((grop=sysrap OR group=soft4soft) AND
45661244<MSN<45661412) OR count<1;
modify:user=yuji OR user=hata OR
IC#card=1afd234fe4def458c3bac78497bbda6f;
print:group=sysrap;
```

のようなACLを設定することができる。

【0070】この設定されたACLによれば、「read」は閲覧条件を示し、グループが「sysrap」あるいは「soft4soft」であり、かつ、メディアシリアル番号MSNが45661244を越え45661412未満であるか、あるいは操作済回数が1未満すなわち、一度もコンテンツを利用したことがないことが閲覧のための条件となる。さらに、「modify」は更新条件を示し、ユーザ名が「yuji」あるいは「hata」であるか、あるいは「IC#card」の番号が「1afd234fe4def458c3bac78497bbda6f」であることがコンテンツ更新のための条件となる。

【0071】また、「print」は印刷出力条件を示し、グループが「sysrap」に限り、コンテンツを印刷することができる。このようなACLは、著作権者システム20から著作権者1が任意に設定することができる。このACL設定は、GUIを用いることによって操作性が向上する。なお、ACLのタイプは、操作名とともに設定するようにしてもよい。たとえば、操作名1に対してはアクセス条件(1)なる条件を選択でき、操作名2に対してはアクセス条件(2)なる条件を選択できるようにしてもよい。これにより、さらに操作性が向上する。

【0072】つぎに、図4に示すフローチャートを参照して、コンテンツサーバ30の内部処理手順について説明する。図4において、まずコンテンツサーバ30は、ネットワークイベントが入力されたか、入力された場合

に秘匿コンテンツ登録要求か、秘匿コンテンツ配布要求かを判断する(ステップS200)。ネットワークイベントが入力されない場合(ステップS200、なし)には、ステップ200における判断処理を繰り返す。

【0073】ネットワークイベントが秘匿コンテンツ登録要求である場合(ステップS200、秘匿コンテンツ登録要求)には、この登録要求された秘匿コンテンツを内部登録し(ステップS210)、デフォルトのACLを設定する(ステップS211)。そして、著作権者システム20に、この秘匿コンテンツ登録要求に対する応答を行って(ステップS212)、ステップS200に移行し、上述した処理を繰り返す。

【0074】一方、ネットワークイベントが秘匿コンテンツ配布要求である場合(ステップS200、秘匿コンテンツ配布要求)には、この配布要求された秘匿コンテンツを利用者システム50に対して配布し(ステップS220)、その後、この秘匿コンテンツ配布要求に対する応答を利用者システム50に対して行い(ステップS221)、ステップS200に移行して上述した処理を繰り返す。これにより、コンテンツサーバ30を介して秘匿コンテンツを秘密状態で著作権者システム20から利用者システム50に配布することができる。この場合、トラフィックが分散され、高速転送が可能であるとともに、予め利用者システム50の近傍のコンテンツサーバまで秘匿コンテンツを保持することが可能であるので、配布処理を高速に処理することができる。

【0075】つぎに、図5に示すフローチャートを参照して、ライセンスサーバ40の内部処理手順について説明する。図5において、まず、ライセンスサーバ40は、コンテンツ利用要求のネットワークイベントが入力されたか否かを判断する(ステップS300)。ネットワークイベントが入力されない場合(ステップS300、なし)には、このステップS300の判断処理を繰り返す。

【0076】ネットワークイベントがコンテンツ利用要求である場合(ステップS300、コンテンツ利用要求)には、指定されたコンテンツのACLをLDAPシステム42から検索し(ステップS301)、さらに、この検索したACLから関連するアクセス条件を抽出し、新たなACLを生成する(ステップS302)。その後抽出した物理環境特定条件に対応する対応物理要素ID証明書があるか否かを判断し(ステップS303)、対応物理要素ID証明書がある場合(ステップS303、対応物理要素ID証明書あり)にはそのまま、対応物理要素ID証明書が無い場合(ステップS303、対応物理要素ID証明書無し)には、コンテンツの利用要求者に対して、すなわち利用者システム50に対して証明書を要求した(ステップS304)後、さらに、つぎの物理環境特定条件があるか否かを判断する(ステップS305)。

【0077】つぎの物理環境特定条件がある場合（ステップS305、あり）には、ステップS303に移行して対応物理要素ID証明書を確実に備える準備をし、つぎの物理環境特定条件がない場合（ステップS305、なし）には、コンテンツの利用要求者、すなわち利用者システム50から物理要素ID証明書群を受信する（ステップS306）。

【0078】その後、ライセンス許可／生成部41は、指定されたコンテンツ復号キーを検索し（ステップS307）、ACL内のアクセス条件を、強制可能な物理要素の証明書に並べ直す（ステップS308）。さらに、ACL内のすべてのAND/OR式を認証優先順に括弧でくくる処理を行う（ステップS309）。その後ライセンス許可／生成部41は、この括弧でくくられたAND/OR式をもとに、ライセンスを生成するライセンス生成処理を行う（ステップS310）。そして、生成されたライセンスを利用者システム50に送信し（ステップS311）、ステップS300に移行して上述した処理を繰り返す。

【0079】ここで、生成されたライセンスと秘匿コンテンツとの関係について図6を参照して説明する。図6は、ライセンスサーバ40から利用者システム50に送信されるライセンスとコンテンツサーバ30を介して著作権者システム20から利用者システム50に送信される秘匿コンテンツとの関係を示している。

【0080】図6において、ライセンスサーバ40のACL43内には、それぞれ各秘匿コンテンツ71～75と対応づけられたシステムACL43-1～43-5が格納されている。このシステムACLをもとにその後、たとえば秘匿コンテンツ71～73に対応するシステムACLから秘匿コンテンツ71～73に対するライセンス84～86が生成され、利用者システムに送信される。このライセンス84～86は、対応する物理要素IDで暗号化されており、外部に情報が漏れることはない。利用者システム50は、ライセンス84～86からクライアントACL81～83を復号し、これらに対応する秘匿コンテンツ71'～73'を復号し、それぞれコンテンツを得ることができる。

【0081】この場合、秘匿コンテンツも暗号化されているので、セキュリティは十分である。このようにして、ACLと秘匿コンテンツとはその秘匿状態を維持しながら、それぞれ転送ルートが異なるものの、対応づけられている。なお、コンテンツサーバ30を含む転送経路を介して送られる秘匿コンテンツの状態は、仮想格納領域70として表現している。

【0082】ここで、さらにライセンスサーバ40内のLDAPシステム42について図7を参照して説明する。図7において、LDAPシステム42は、複数のLDAPサーバを有し、そのクライアントサーバとしてライセンスサーバ40が位置づけられ、ライセンスサーバ

40の管理のもとに各LDAPサーバが機能することになる。LDAPサーバとは、ディレクトリサービスの標準であるX.500に含まれるDAPの軽量版のプロトコルを用いたディレクトリサーバである。LDAPサーバ内には複数のクラスに分けられ、たとえば個人情報91、システムクラス92、メディアクラス93、XMLで記述されたXML情報のクラスを有する。

【0083】そして、たとえば個人情報91のクラスにおいて、「own system」が検索されると、このシステムをシステムクラス92から「system name」によって検索し、さらにシステムクラス92内の現メディア「current media」は、メディアクラスの中からメディアクラス93を検索し、さらに、このメディアクラス93内のコンテンツから、このコンテンツに対応したXML情報94を検索することができる。このXML情報94の中には、コンテンツに関する情報が格納されている。

【0084】ところで、利用者システム50の特定利用環境は、図8に示すレイヤを持った論理構造を有している。図8では、特定利用環境100が、アプリケーション層110とOSカーネル層111とデバイス層112との3層で構成され、各層間は、点線で示すサービスインターフェースで接続される。アプリケーション層110は、コンテンツ再生・実行アプリケーション101を有し、内部には、秘密コンテンツ復号保護ライブラリ102をプログラムモジュールとして有する。

【0085】秘密コンテンツ復号保護ライブラリ102は、ストレージドライバ103、ファイルシステム105、複数の利用環境特定物理要素ドライバ106～108、再生デバイスドライバを動作させる。ストレージドライバ103は、コンテンツストレージデバイスを駆動させ、利用環境特定物理要素ドライバ106～108はそれぞれ利用環境特定物理要素109～111を駆動させ、再生デバイスドライバ112は再生デバイス113を駆動させる。なお、一つの物理装置であっても、たとえばMO装置のようにコンテンツストレージデバイス104と利用環境特定要素109の二つの役割を担ってもよい。

【0086】図9は、利用環境特定物理要素（PCSUE）のOSカーネル層111とデバイス層112との対応関係を示している。図9に示すように、PCSUE同士は、包含関係を持つことがある。もちろん、デバイス層112における他のデバイスも同様である。たとえば、PCSUE131の下位にはPCSUE133、134が位置づけられ、PCSUE134の下位にはPCSUE135、136が位置づけられる。このような包含関係を有するPCSUE同士では、物理要素ID等の情報をデータ交換することができる。

【0087】たとえば、DVD装置等のメディア再生装置のPCSUEは、DVD等のメディアのPCSUEを包含しており、コンテンツデータやメディアID情報を

両者間で交換する。たとえば、PCSUE134とPCSUE135との間の情報交換である。そして、最上位のPCSUEのみがPCSUEドライバとのデータ交換を行う。たとえば、PCSUEドライバ120とPCSUE131との関係である。従って、同じデバイス層であっても、包含関係を有し、階層的な関係を有する場合がある。

【0088】ライセンスは、上述したように、特定環境に対する許諾情報であり、ライセンスを要求したクライアント環境、すなわち利用者システムの環境に固有の情報のみを含むものであり、ACLとコンテンツ復号キー K_0 とからなるアクセス情報を物理要素ID (PCSUE-ID) によって暗号化されたものである。

【0089】ここで、多重化されたライセンスの一例を示すと、つぎのようになる。すなわち、

【数1】

$$\{ \{ \{ \{ \{ \langle \text{アクセス情報} \rangle \mid K_5 \mid K_4 \mid K_3 \mid K_2 \mid K_1 \} \} \} \}$$

である。ここで、 $K_1 \sim K_5$ は、それぞれPCSUE-IDである。このライセンスは、アクセス情報は $K_1 \sim K_5$ を用いてAND条件によって結合されている。物理要素のセキュリティ強度が高い順に各PCSUE-IDを用いて多重的に暗号化するとよい。この復号化は、この逆に外側のPCSUE-IDから順次復号されることになる。

【0090】また、物理要素のセキュリティ強度がほぼ同一の場合には、各PCSUE-IDを排他的論理和演算によってその結果の暗号キーによって復号できるようにしてもよい。たとえば、

【数2】

$$\{ \langle \text{アクセス情報} \rangle \mid (K_5 \oplus K_4 \oplus K_3 \oplus K_2 \oplus K_1) \}$$

のようにするとよい。これらの暗号化の多重化によって、一部の製品、すなわち一部の物理要素への攻撃成功によるコンテンツ復号キー K_0 盗難の危険性が分散されるという、リスク分散の効果をもたらすことになる。

【0091】また、複数のPCSUE-IDをOR演算子で結合する場合、すなわち、

【数3】

$$\begin{aligned} & \{ \langle \text{アクセス情報} \rangle \mid K_5 \mid \langle \text{アクセス情報} \rangle \mid K_4 \mid \\ & \langle \text{アクセス情報} \rangle \mid K_3 \mid \langle \text{アクセス情報} \rangle \mid K_2 \mid \\ & \langle \text{アクセス情報} \rangle \mid K_1 \} \end{aligned}$$

のような場合には、それぞれのPCSUE-IDで暗号化されたサブライセンス、たとえば、 $\{ \langle \text{アクセス情報} \rangle \mid K_1 \}$ を生成し、すべてのサブライセンスを単純にOR演算して結合した値をライセンスとしてもよい。この場合、上述した暗号化の多重化を各サブライセンスにも適用し、AND、XOR、OR演算を入れ子にして組み合わせたライセンスとして生成してもよい。これによっ

ても、リスク分散の効果は得られる。

【0092】つぎに、このようなライセンスの生成処理手順について図10に示すフローチャートを参照して説明する。この図10に示すフローチャートは、図5のステップS310に示すライセンス生成処理手順のサブルーチンである。図5において、まず、上述したACLから1ワード読み出す(ステップS400)。その後読み出したワードが「(」であるか否かを判断する(ステップS410)。

【0093】読み出したワードが「(」である場合(ステップS410、「(」)には、ACLの読み出し現在位置を括弧内ACLの始点として記憶する(ステップS411)。その後、変数NBを「0」に設定し(ステップS412)、さらにACLから1ワード読み出す(ステップS413)。その後、読み出したワードが「(」であるか否かを判断し(ステップS414)、「(」である場合には、変数NBに「1」を加算した(ステップS415)後、ステップS413に移行して再び、つぎの1ワードを読み出す。

【0094】一方、読み出しワードが「(」でない場合(ステップS414、その他)には、さらにこの読み出したワードが「)」であるか否かを判断する(ステップS416)。この読み出したワードが「)」でない場合、すなわちその他である場合には、ステップS413に移行し、さらにACLから1ワードを読み出す。一方、この読み出したワードが「)」である場合には、NBが「0」であるか否かを判断する(ステップS417)。NBが「0」でない場合(ステップS417、NO)には、NBの値から「1」減算し、ステップS413に移行し、さらにACLから1ワード読み出す。

【0095】NBが「0」のとき(ステップS417、YES)には、ACLの現在位置の一つ手前を括弧内ACLの終点として記憶する(ステップS419)。その後、この括弧内ACLのライセンス生成処理を行い(ステップS420)、その再帰呼び出しによる戻り値をアクセス条件ACに追加する処理を行って(ステップS421)、ステップS400に移行する。これによって括弧内のACLが生成される。

【0096】一方、読み出したワードが「(」でない場合(ステップS410、その他)には、さらに、この読み出したワードが物理要素条件または会計条件であるか否かを判断する(ステップS410)。物理条件または会計条件である場合には、この条件をアクセス条件ACに設定し(ステップS431)、この条件を強制可能な物理要素の秘密キー K_p として設定し(ステップS432)、ステップS400に移行し、さらにACLから1ワード読み出す。

【0097】読み出したワードが物理条件または会計条件でない場合(ステップS410、その他)には、さらに、この読み出したワードが「OR」であるか否かを判

断する(ステップS430)。読み出したワードが「OR」である場合には、この読み出したワードから後のACLのライセンス生成処理を行う(ステップS441)。その後、さらに生成したライセンスの中にACが含まれるか否かを判断し(ステップS442)、ACが含まれる場合(ステップS442、YES)には、ステップS441によるライセンス生成処理の戻り値を用いて「{AC, hash} Kp, 戻り値」となるライセンスに設定し(ステップS443)、この生成したライセンスを返す(ステップS454)。一方、ライセンスの中にACが含まれていない場合(ステップS442、NO)には、ステップS441によるライセンス生成処理の戻り値を用いて「{Kc, AC, hash} Kp, 戻り値」となるライセンスに設定し(ステップS445)、この生成したライセンスを返す(ステップS454)。

【0098】一方、読み出したワードが「OR」でない場合(ステップS430、その他)には、さらに、この読み出したワードが「AND」であるか否かを判断する(ステップS440)。読み出したワードが「AND」である場合には、この読み出したワードから後のACLのライセンス生成処理を行い(ステップS452)、このライセンス生成処理の戻り値を用いて「[戻り値, AC, hash] Kp」となるライセンスを返す(ステップS454)。

【0099】さらに、この読み出したワードが「AND」でない場合(ステップS440、その他)には、「{Kc, AC, hash} Kp」となるライセンスを返す(ステップS454)。これにより、ACLからライセンスが生成される。

【0100】つぎに、図11に示すフローチャートを参照して、利用者システム50の内部処理手順について説明する。図11において、まず利用者システム50は、コンテンツの利用要求があったか否かを判断する(ステップS500)。コンテンツの利用要求がない場合(ステップS500、なし)には、この判断処理を繰り返す、コンテンツの利用要求があった場合(ステップS500、あり)には、コンテンツの利用要求を送信する(ステップS501)。その後、物理要素の証明書の要求がライセンスサーバ40からあったか否かを判断し(ステップS502)、物理要素の証明書の要求がない場合(ステップS502、なし)には、ステップS508に移行する。

【0101】一方、物理要素の証明書の要求があった場合(ステップS502、あり)には、物理要素ID証明書を読み出し(ステップS503)、読み出し失敗したか否かを判断する(ステップS504)。読み出しに失敗した場合(ステップS504、YES)には、エラー通知をライセンスサーバに送信して(ステップS505)、ステップS500に移行する。一方、読み出しに失敗しない場合(ステップS504、NO)には、つぎ

の物理要素があるか否かを判断し(ステップS506)、つぎの物理要素がある場合(ステップS506、あり)には、ステップS503に移行して、つぎの物理要素ID証明書の読み出しを行って上述した処理を繰り返す。

【0102】一方、つぎの物理要素がない場合(ステップS506、なし)には、物理要素ID証明書をライセンスサーバ40に送信し(ステップS507)、さらに受信内容がエラーかライセンスかを判断する(ステップS508)。受信内容がエラーである場合(ステップS508、エラー)には、ステップS500に移行して上述した処理を繰り返す、受信内容がライセンスである場合(ステップS508、ライセンス)には、さらに、ライセンスを物理要素(PCSUE)1に渡し(ステップS509)、ステップS500に移行して上述した処理を繰り返す。これにより、利用者システム50は、ライセンスサーバ40からライセンスを取得することができる。

【0103】ここで、PCSUE1とは、(N-1)個のPCSUEの最初のPCSUEを示し、一般的にPCSUEIで示し、Iは、1~(N-1)の整数である。そこで、各PCSUEIがライセンスを渡された時の内部処理手順について図12のフローチャートを参照して説明する。

【0104】図12において、まずPCSUEIは、受信したライセンスをKpiで復号する(ステップ600)。その後、この復号したアクセス条件ACIを評価し(ステップS601)、アクセス条件ACIの評価結果が可か不可かを判断する(ステップS602)。アクセス条件ACIの評価結果が不可の場合(ステップS602、不可)には、エラー処理を行って(ステップS604)、本処理を終了する。一方、アクセス条件ACIの評価結果が可である場合(ステップS602、可)には、この復号したライセンスをPCSUE(I+1)に送信し、復号を続行させ、本PCSUEIの内部処理を終了する。

【0105】つぎに、PCSUE(I+1)は、PCSUE(N)に相当し、ここでは、たとえば、再生デバイスの物理要素が内部処理を行う。この内部処理手順について図13に示すフローチャートを参照して説明する。図13において、まず、受信したライセンスをKpnで復号する(ステップS700)。その後、この復号したアクセス条件AC(N)を評価し(ステップS701)、この評価結果が可であるか、不可であるかを判断する(ステップS702)。評価結果が不可である場合(ステップS702、不可)には、エラー処理を行って(ステップS703)、本処理を終了して、結果的に秘匿コンテンツを復号することができないことになる。

【0106】一方、アクセス条件AC(N)に対する評価結果が可である場合(ステップS702、可)には、

この復号したKcで秘匿コンテンツを復号し（ステップS704）、復号したコンテンツを再生デバイスが再生し（ステップS705）、本処理を終了する。

【0107】ここで、具体的なライセンスの復号処理を図14を参照して説明する。図14において、ライセンスサーバ40で生成されたライセンスは、アクセス制御リストACLとコンテンツ復号キーとを再生デバイス144の物理要素IDであるキーKpを用いて暗号化し、さらに、ストレージデバイスのデバイスシリアル番号であるDSN141とメディア142のメディアシリアル番号であるMSN143の排他的論理和の値をキーとして暗号化されたものである。

【0108】まず、ストレージデバイス140は、メディア142に書き込み不可のMSNを読み込み、この値とストレージデバイス140自身のDSNとの排他的論理和の演算を行い、この演算結果によってライセンスを復号すると、ライセンスは、{ACL, Kc} Kpとなる。この一部復号されたライセンスは、再生デバイス144に送られ、再生デバイス144は、再生デバイス144自身が有する物理要素IDであるキーKpを用いてライセンスを復号し、アクセス条件リストACLとコンテンツ復号キーKcとを取得し、アクセス条件ACLが示すアクセス条件を満足する場合に、コンテンツ復号キーKcによって復号を行うことができ、復号されたコンテンツは、再生デバイス144によって再生されることになる。

【0109】上述したライセンス要求とライセンス取得によるコンテンツ復号処理を図15に示すデータフローを参照してさらに説明する。図15において、利用者システム50内における復号保護領域では、まずコンテンツを利用するためライセンス要求処理152を物理要素ID証明書を付してライセンスサーバ40に送出する。この際、物理要素ID証明書は、利用環境特定物理要素証明書取得処理153によって利用環境特定物理要素150から取得され、ライセンス要求処理152によって渡される。

【0110】一方、ライセンスサーバ40からライセンスが送信されるとライセンス取得処理156は、このライセンスを取得し、アクセス許可処理155は、ライセンス所得処理156からライセンスを取得するとともに、利用環境特定物理要素ID認証処理154が利用環境特定物理要素証明書取得処理153を介して物理要素IDを取得し、さらに会計処理157から利用状況を取得し、これらを用いて復号キーを取り出す。

【0111】そして、コンテンツ復号処理159は、コンテンツ復号キーを用いて秘匿コンテンツ158を復号し、平文のコンテンツを出力する。なお、会計処理157は、利用状況監視物理要素151に通知し、利用環境監視物理要素151によって現在の利用状況が利用に応じて自動的にデクリメントされる。

【0112】ところで、図16は、図8に示した特定利用環境の各エンティティに各処理手続きを実装した場合の保護強度への影響を示す図である。この結果から、利用環境特定物理要素所有証明書の生成は、デバイス層に実装し、会計情報保護は、ICカードによるデバイス層に実装することが好ましいことがわかる。このように、各処理手続きを実装するレイヤによっても保護強度が異なるので、レイヤ配置も考慮して図15に示す各処理機能を実装する必要がある。

【0113】なお、上述した実施の形態では、いわゆるコンテンツキャッシュ可能型モデルを基準とした構成として説明したが、これに限らず、コンテンツ同時配布型モデルを基準とした構成にも適用できるのは明らかである。この場合、コンテンツサーバ30がライセンスサーバ40内に内部配置された構成として取り扱えばよい。

【0114】さらに、上述した実施の形態では、暗号化、復号化に関して、キーを用いることが前提となっているが、この場合において、秘密鍵暗号方式を用いても、公開鍵暗号方式を用いても、いずれでも実施可能であり、適応されるシステムに応じてそれぞれ適切な方式を適用すればよい。

【0115】また、上述した実施の形態に示す物理要素には、利用者システム50に固定の装置のみではなく、この利用者システム50を利用する際に用いられるメディア、すなわちCD-ROM、DVD、MO、ICカードやフロッピーディスク等の可搬型の記録媒体を含むものである。この可搬型の記録媒体が用いられる利用者システムにおいては、この利用者システムに固定の物理要素に加えて、この用いられる可搬型の記録媒体も物理要素に含まれて、コンテンツの利用制御がなされることになる。なお、利用者システム50に固定のメディア、例えば固定のハードディスク装置や固定のROM等が上述した物理要素に含まれるのは言うまでもない。

【0116】

【発明の効果】以上説明したように、請求項1にかかる発明によれば、設定手段が、前記利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件として設定し、前記利用制御手段は、前記設定手段によって設定された利用許可条件をもとに前記利用者手段による前記コンテンツの利用を制御し、利用許可条件に基づいた柔軟な利用制御を可能とするようにしているので、この利用許可条件に基づいた柔軟なコンテンツ利用制御を行うことができるという効果を奏する。

【0117】また、請求項2にかかる発明によれば、設定手段によって設定される部分利用許可条件は、前記利用者手段および前記利用者の利用状況に応じて変化する力

テゴリーに対する条件である会計条件を含むようにしている、一層利用者に対するコンテンツ利用制御を細かにかつ柔軟に行うことができるという効果を奏する。

【0118】また、請求項3にかかる発明によれば、生成手段が、前記利用者手段からのコンテンツ利用要求を受けて、前記利用許可条件および前記コンテンツの復号キーを前記利用者手段内で使用するメディアを含む当該利用者手段の複数の物理要素に関する識別情報によって暗号化した許諾情報を生成し、前記利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うようにしているので、保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【0119】また、請求項4にかかる発明によれば、利用許可条件内の部分利用許可条件間が論理積で記述されている場合には、当該部分利用許可条件に対応する物理要素の識別情報による暗号化を多重化して行っている、一部の物理要素に対する攻撃成功によるコンテンツ復号キーの盗難の危険性を分散することができるという効果を奏する。

【0120】また、請求項5にかかる発明によれば、物理要素が包含関係にある物理要素であっても一つの物理要素として取り扱っているので、この一つの物理要素の不正も許さず、コンテンツ復号キーの盗難という危険性を分散することができるという効果を奏する。

【0121】また、請求項6にかかる発明によれば、開放ネットワーク上に、前記情報提供権限者手段によって暗号化したコンテンツを保持し、前記利用者手段からのコンテンツ配布要求を受け付けて前記暗号化したコンテンツを当該利用者手段に送付するコンテンツサーバを有しているので、開放ネットワークを十分に活用して当該システムにおけるトラフィックの輻輳を防止して、迅速にコンテンツを獲得することができるという効果を奏する。

【0122】また、請求項7にかかる発明によれば、設定手段が、利用者手段内で使用するメディアを含む当該利用者手段の物理要素に関する識別情報および前記利用者に関する識別情報に基づいた前記コンテンツに対する複数の部分利用許可条件をさらに論理和および論理積の組み合わせによって構造化表現した利用許可条件を前記利用制御手段内の条件格納手段に格納することによって予め設定するとともに、保持手段に前記コンテンツの復号キーを保持する。抽出手段は、前記利用者手段からのコンテンツの利用要求を受け付けて当該利用者手段に対応する利用許可条件および前記コンテンツの復号キーを抽出し、前記利用者手段から送付された物理要素の識別情報をもとに前記利用許可条件および前記コンテンツの復号キーを暗号化した許諾情報を生成して当該利用者手

段に送出する。利用者手段は、前記コンテンツ利用要求に応じて送られる前記許諾情報を当該利用者手段による物理要素の識別情報をもとに復号し、前記利用許可条件を満足する場合に前記コンテンツの復号キーを用いて前記暗号化されたコンテンツの復号を行うようにしているので、柔軟なコンテンツ利用制御に伴う暗号化、復号化を具体的に実現することができるという効果を奏する。

【0123】また、請求項8、9にかかる発明によれば、要求手段が、コンテンツの利用要求に応じて、コンテンツの管理を行うコンテンツ管理装置に、当該コンテンツ利用装置の物理要素に関する識別情報および利用者に関する識別情報を送信すると、その後、前記コンテンツの利用要求に対応してコンテンツ管理装置によって送信される許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、前記求めた利用許可条件を判定し許可される場合に前記求めた復号キーを用いてコンテンツの復号を行うようにしているので、保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【0124】また、請求項10、11にかかる発明によれば、まず、コンテンツの利用要求に対応して、コンテンツの許諾情報から、当該コンテンツ利用装置の物理要素に関する識別情報をもとに復号して利用許可条件およびコンテンツの復号キーを求め、その後、前記求めた利用許可条件を判定し許可される場合に、前記求めた復号キーを用いてコンテンツの復号を行うようにしているので、一層保護強度の高いコンテンツ利用制御を行うことができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図である。

【図2】図1に示した著作権者システム20の内部処理手順を示すフローチャートである。

【図3】会計条件と物理環境特定要素条件との一例を示す図である。

【図4】図1に示したコンテンツサーバ30の内部処理手順を示すフローチャートである。

【図5】図1に示したライセンスサーバ40の内部処理手順を示すフローチャートである。

【図6】ライセンスサーバ40から送られるライセンスと著作権者システム10あるいはコンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図である。

【図7】図1に示したLDAPシステム42の構成を示す図である。

【図8】特定利用環境のレイヤ論理構造を示す図である。

【図9】包含関係をもった物理要素の一例を示す図である。

【図10】ライセンス生成処理手順を示す詳細フローチ

ャートである。

【図 1 1】図 1 に示した利用者システム 50 の内部処理手順を示すフローチャートである。

【図 1 2】利用関係特定物理要素によるライセンス復号処理手順を示すフローチャートである。

【図 1 3】再生デバイスの物理要素によるライセンス復号処理手順を示すフローチャートである。

【図 1 4】ライセンスの復号過程の一例を示す図である。

【図 1 5】ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図である。

【図 1 6】特定利用環境の各エンティティに各処理手続きを突装した場合における保護強度への影響を示す図である。

【図 1 7】従来におけるアクセス制御モデルを示す図である。

【図 1 8】従来におけるアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図である。

【図 1 9】改良したアクセス制御モデルを示す図である。

【図 2 0】従来におけるコンテンツ利用制御システムのコンテンツ配布モデルを示す図である。

【図 2 1】コンテンツキャッシュ可能型モデルを示す図である。

【図 2 2】図 2 1 に示したコンテンツキャッシュ可能型モデルに対応するコンテンツ利用制御システムの概要構成を示す図である。

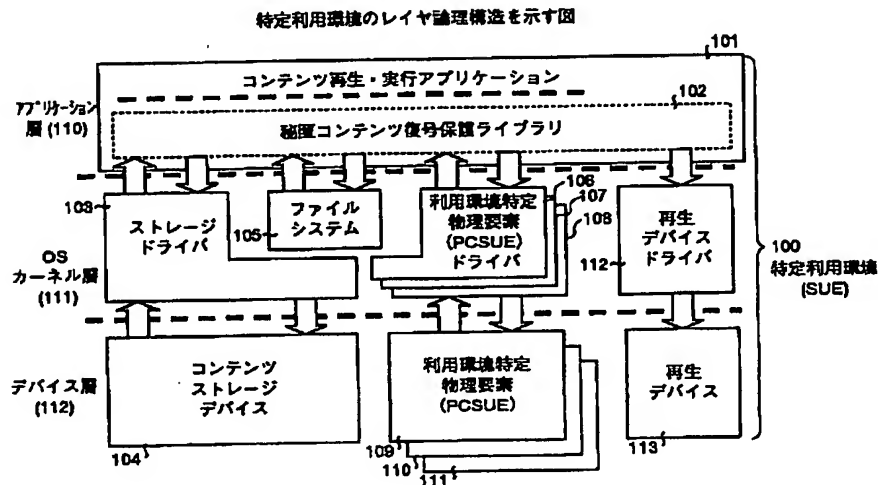
成を示す図である。

【図 2 3】コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図である。

【符号の説明】

- 1 著作権者
- 2 利用者
- 10 コンテンツ利用制御システム
- 20 著作権者システム
- 21 秘密コンテンツ登録部
- 22 アクセス制御権委譲部
- 23 ACL 設定部
- 30 コンテンツサーバ
- 40 ライセンスサーバ
- 41 ライセンス許可／生成部
- 42 LDAP システム
- 43 アクセス制御リスト (ACL)
- 44 キー
- 50 利用者システム
- 51 秘匿コンテンツ要求／取得部
- 52 ライセンス要求／取得部
- 53 特定利用環境
- 54-1～54-N 利用環境特定物理要素
- 55-1～55-M コンテンツストレージデバイス
- 56-1～56-L 再生デバイス
- 57-1、59-1、61-1 物理要素 ID
- 58-1、60-1、62-1 暗号化／復号化／評価部

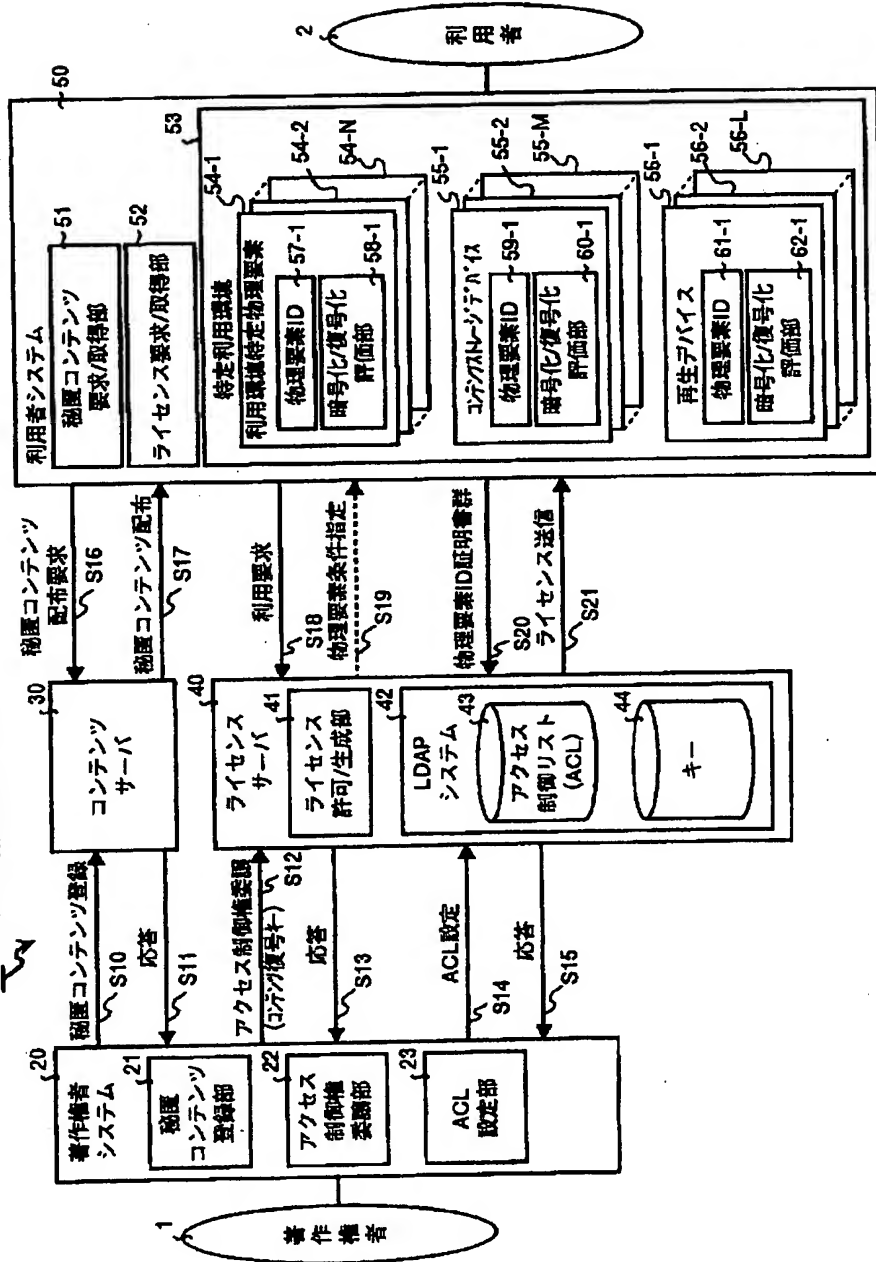
【図 8】



【図1】

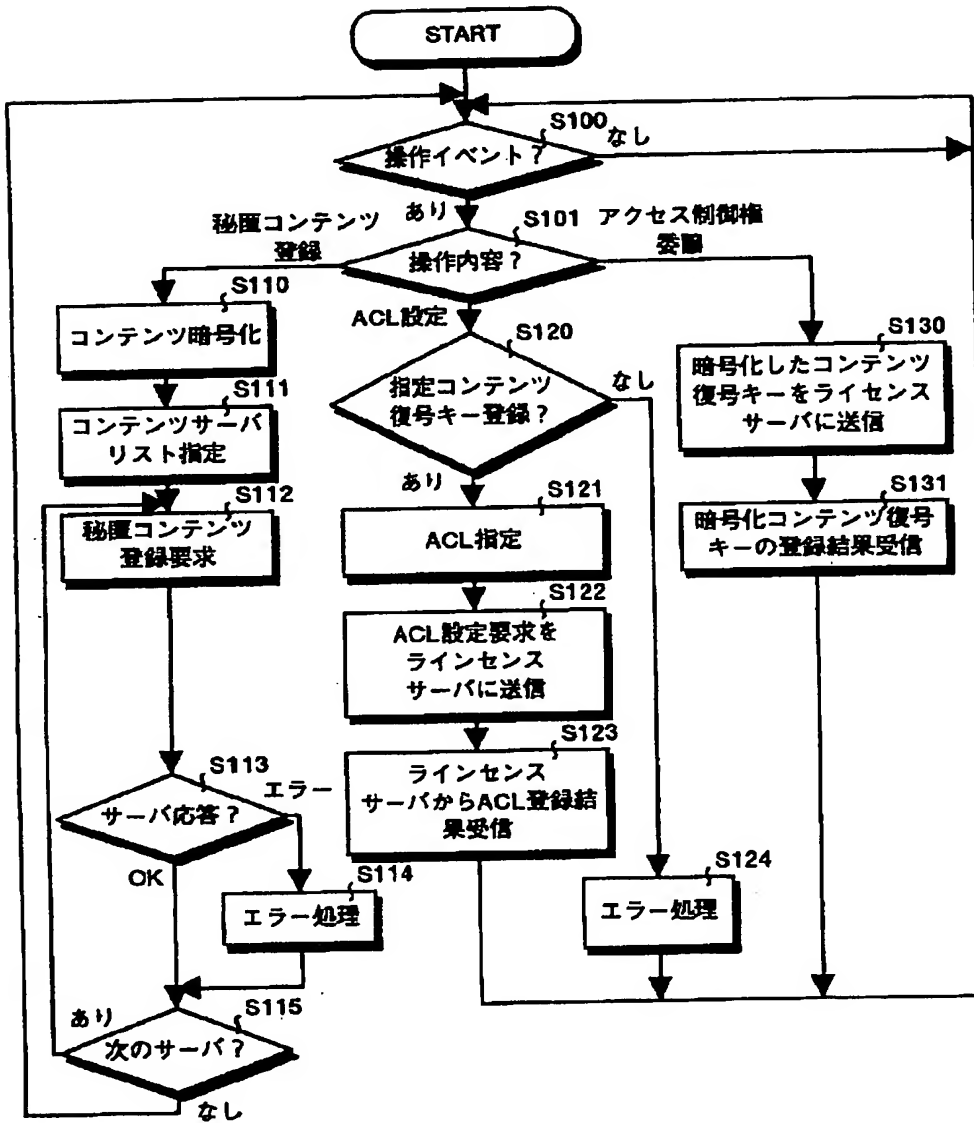
本発明の一実施の形態であるコンテンツ利用制御システムの構成を示す図

10 コンテンツ利用制御システム



【図2】

図1に示した著作権システム20の内部処理手順を示すフローチャート



【図3】

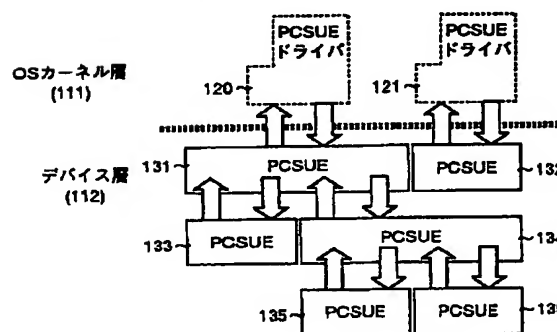
会計条件と物理環境特定要素条件との一例を示す図

| 会計条件値 (Account Condition Value) | 利用状況 (Usage State) |
|---------------------------------|--------------------------------|
| max Count : 操作可能回数最大値 | count : 操作済回数 |
| max Length : 読み出し最大長さ | totalLen : 読み出し済長さ + 被要求読み出し長さ |
| max TimeLen : 実行可能最大時間 | totalTime : 実行済時間長 |
| max Debt : 借入可能金額 (課金条件) | debt : 残金 (マイナスは借入金額) |

| 物理環境特定要素 (PCSUE) 条件 | 物理要素IDクラス (PCSUE-IDClass) |
|---------------------|-----------------------------------|
| (1) 計算機本体 | PSN (プロセッサシリアル番号) |
| (2) 周辺デバイス | DSN : デバイスの種別、シリアル番号 |
| (3) メディア | MSN : メディアの種別、シリアル番号 |
| (4) ICカード | certificates : ICカードが発行する証明書 |
| (5) 人体部位 (指紋、網膜…) | body Parts : 人体部位 (指紋、網膜…) 認証情報 |
| (6) 許可する時間帯 | time Period : 時刻 (ローカルクロック、GPSなど) |
| (7) ネットワークドメイン | MACAddress : MACアドレス |
| (8) 地理的位置 (利用国など) | location : GPS/PHS検出位置 |
| (9) 人の記憶 | user-ID WithPwd : ユーザIDとパスワード |
| (10) グループ | group : 物理要素IDの集合 |

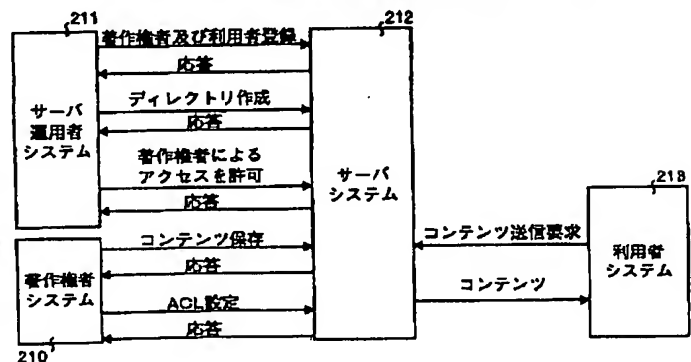
【図9】

包含関係をもった物理要素の一例を示す図



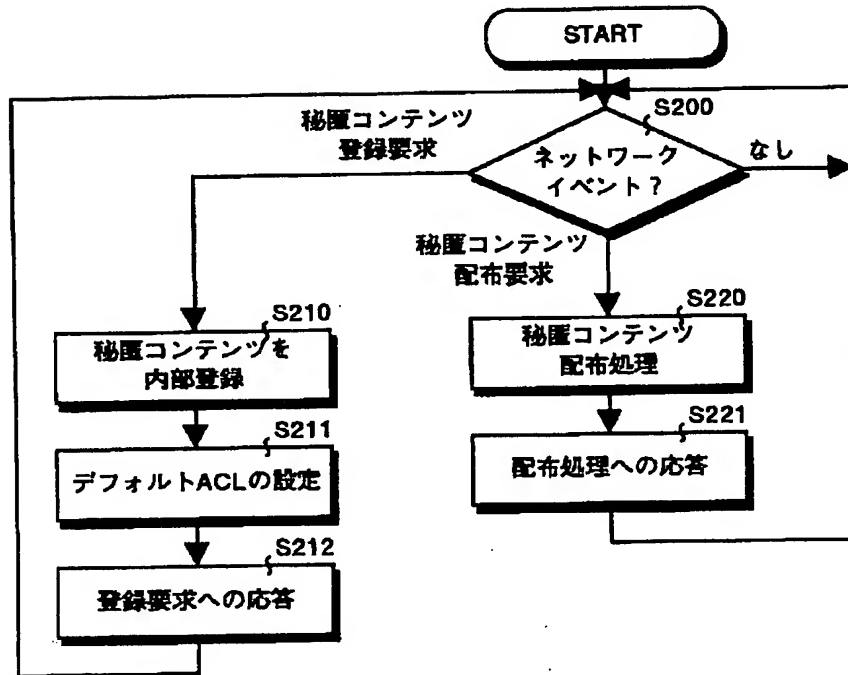
【図18】

従来のアクセス制御モデルに対応したコンテンツ利用制御システムの概要構成を示す図



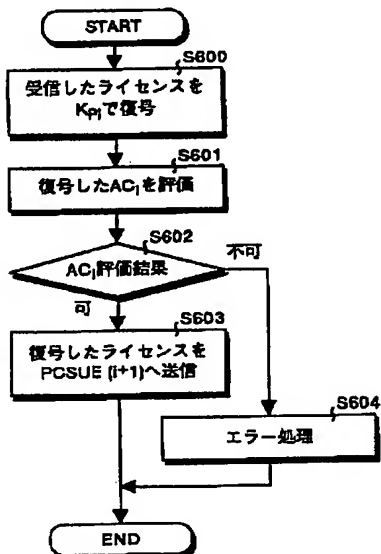
【図4】

図1に示したコンテンツサーバ30の内部処理手順を示すフローチャート



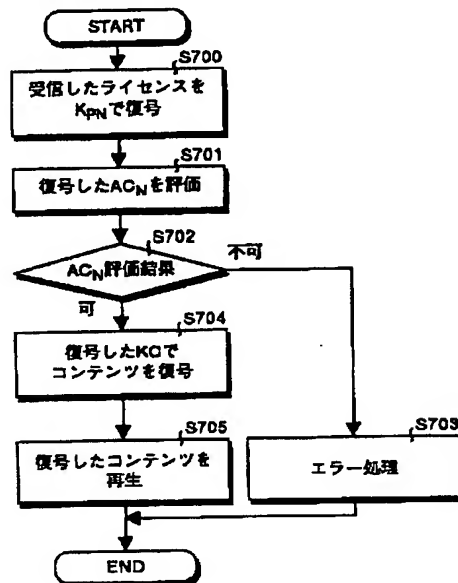
【図12】

利用者関係特定物理要素によるライセンス
復号処理手順を示すフローチャート



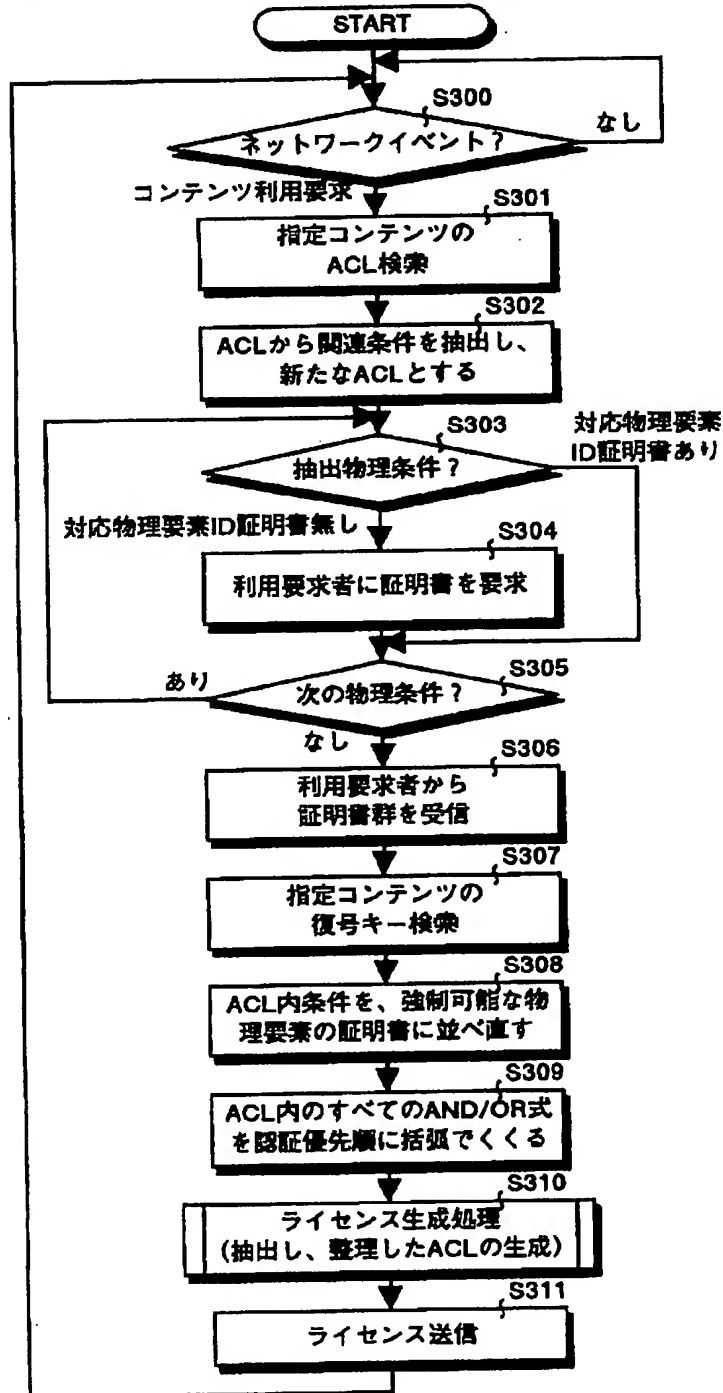
【図13】

再生デバイスの物理要素によるライセンス
復号処理手順を示すフローチャート



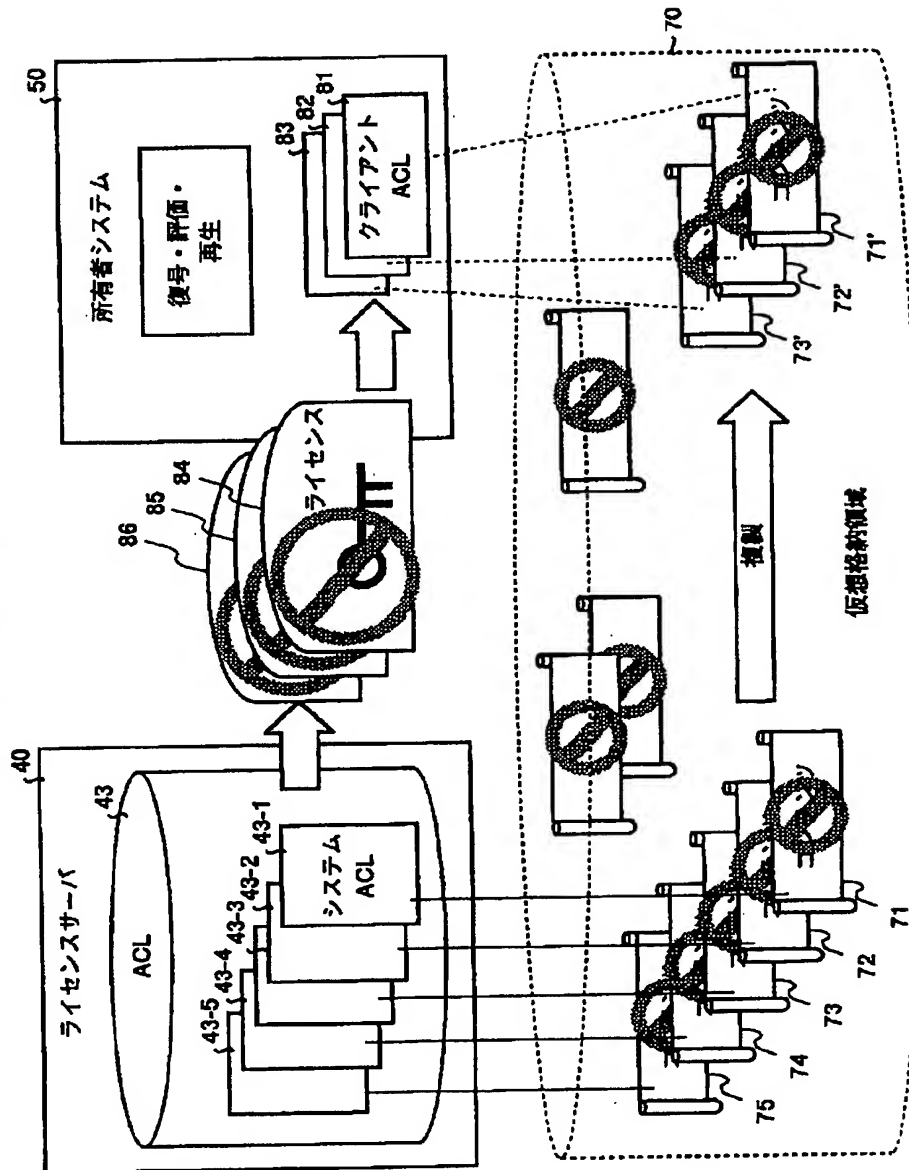
【図5】

図1に示したライセンスサーバ30の内部処理手順を示すフローチャート



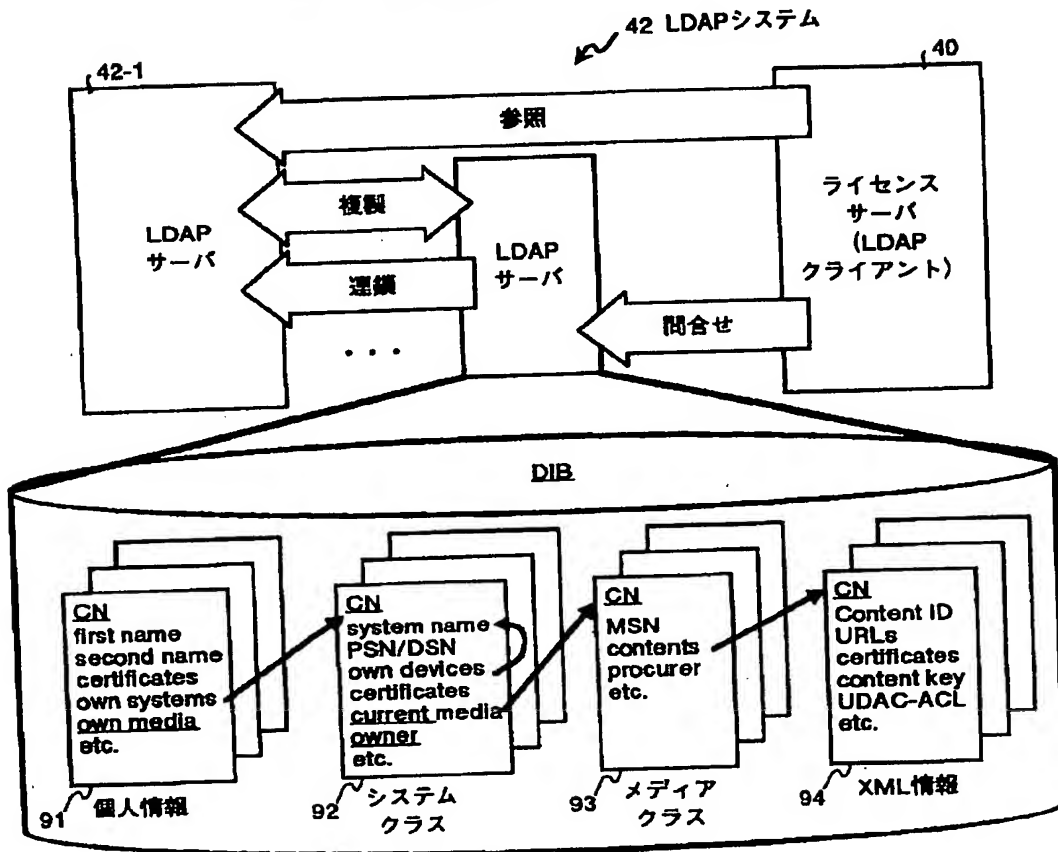
【図6】

ライセンスサーバ40から送られるライセンスと著作権者システム10あるいはコンテンツサーバ30から送られる秘匿コンテンツとの関係を示す図



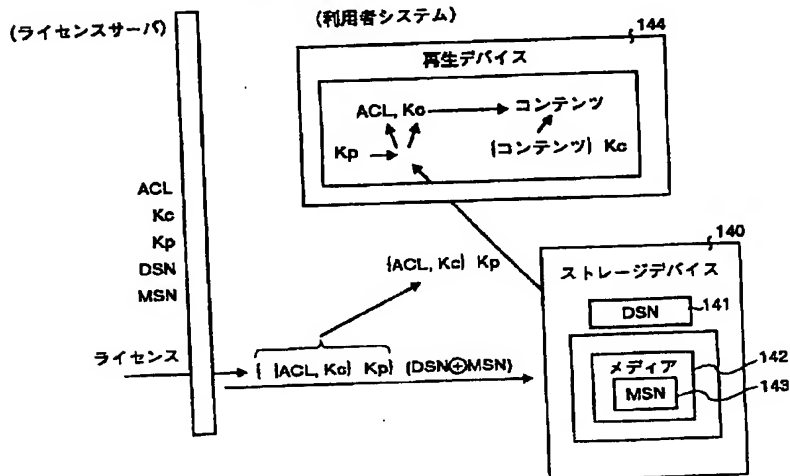
【図7】

図1に示したLDAPシステム42の構成を示す図



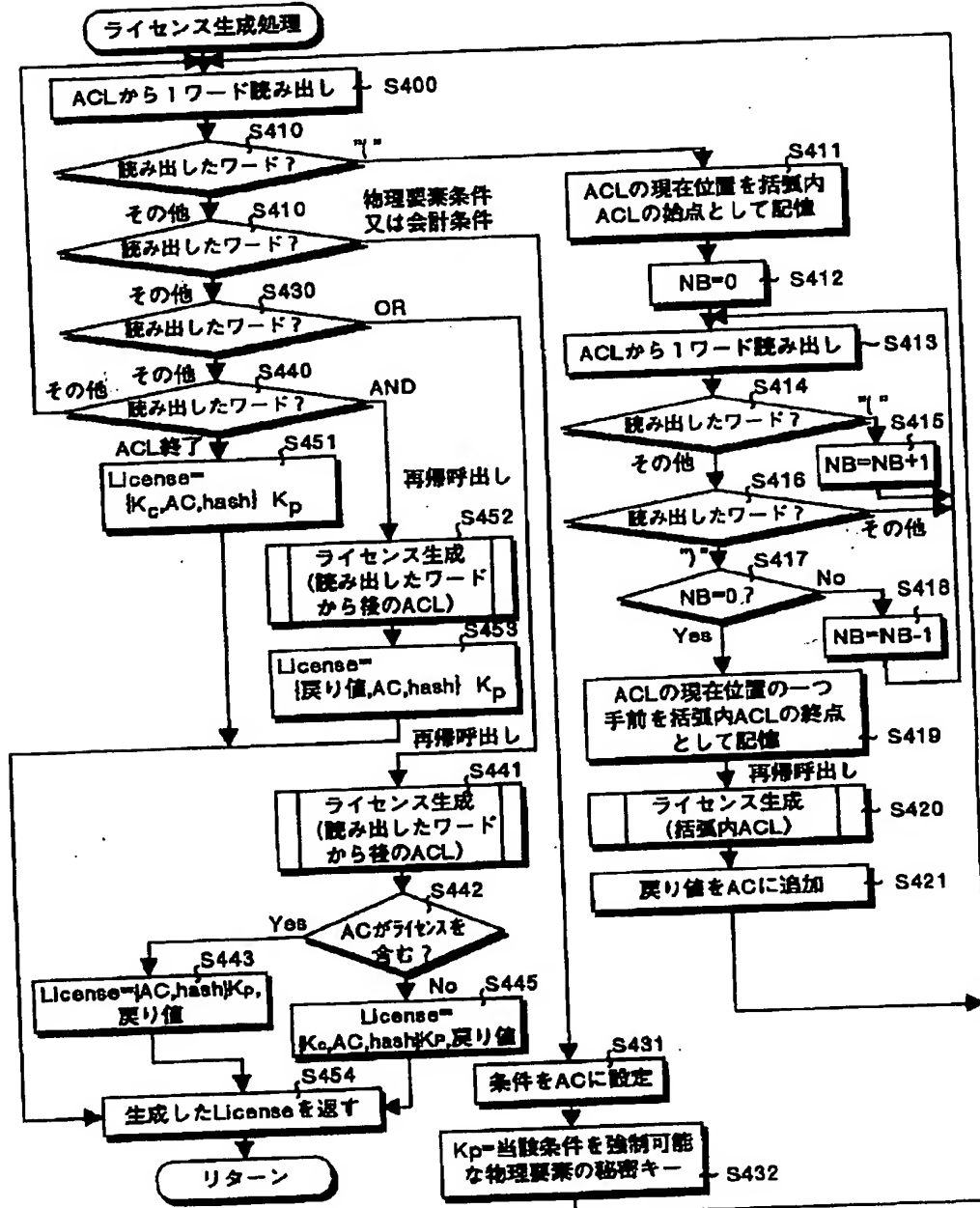
【図14】

ライセンスの復号課程の一例を示す図



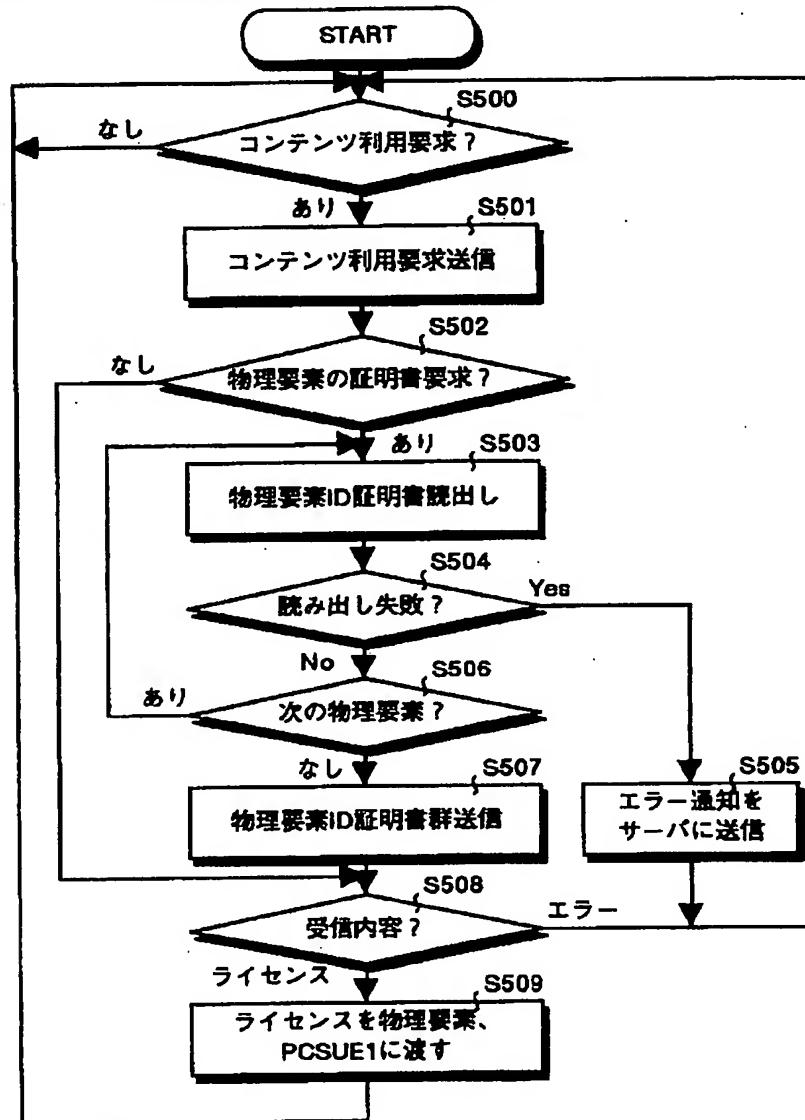
【図10】

ライセンス生成処理手順を示す詳細フローチャート



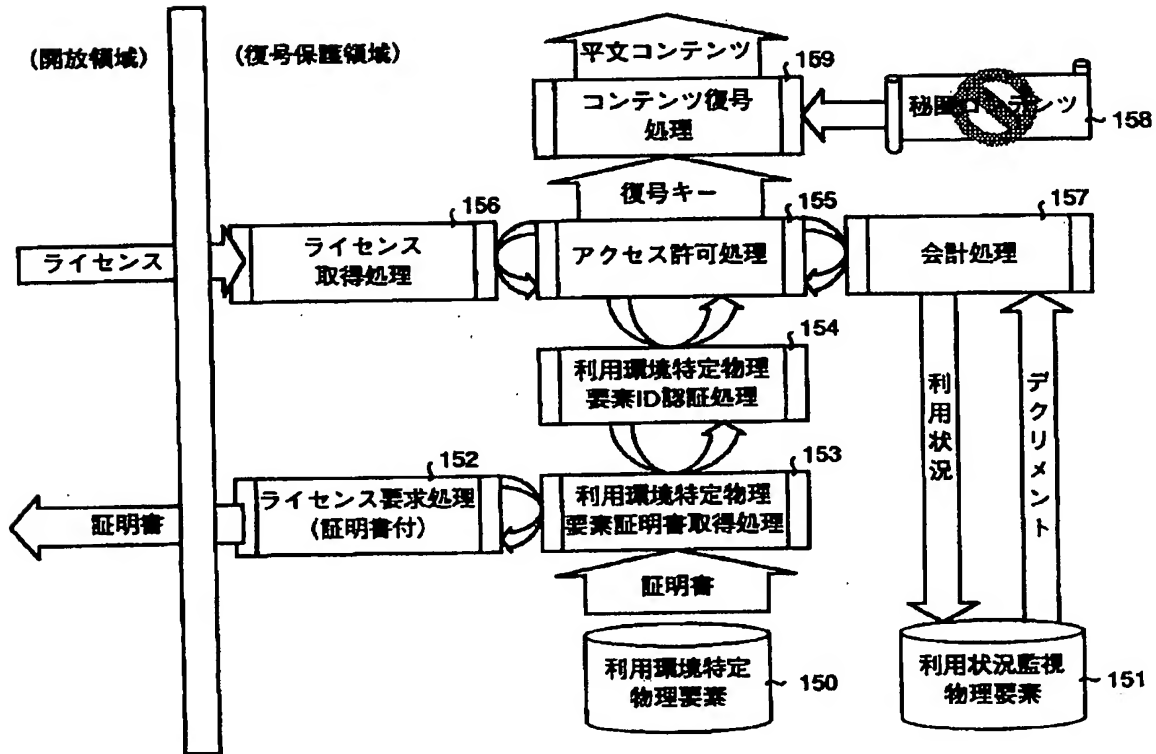
【図11】

図1に示した利用者システム50の内部処理手順を示すフローチャート



【図15】

ライセンス要求とライセンス取得によるコンテンツ復号処理を示すデータフロー図



【図16】

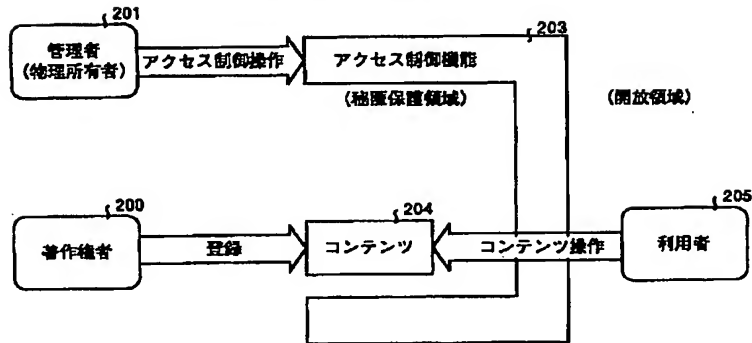
特定利用環境の各エンティティに各処理手続きを実装した場合における保護強度への影響を示す図

| | アプリケーション層 | デバイスドライバ層 | デバイス層 |
|-----------------------|-----------|-----------|-----------|
| 利用環境特定物理要素 所有証明書生成 | — | ○ | ◎ |
| 利用環境特定物理要素 ID認証 | ○ | — | — |
| アクセス制御リスト 検索 | ○ | — | ○ |
| 会計情報保護 | △ | — | ◎ (ICカード) |
| 条件付アクセス許可 | ○ | — | ○ |
| 復号 | ○ | — | ○ |

—: 実装の意義が少ない △: 危険 ○: 専門家には保護が弱い ◎: 保護が強い

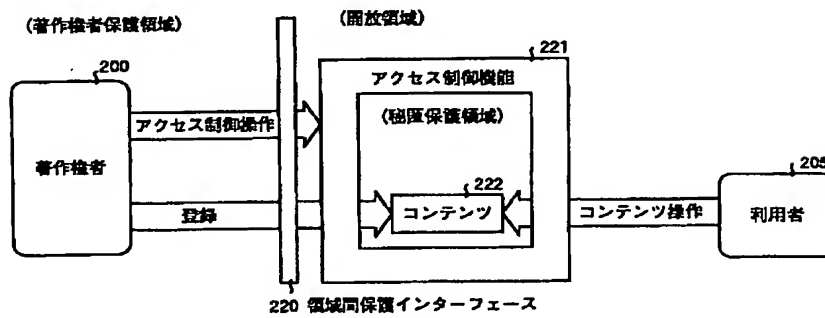
【図17】

従来のアクセス制御モデルを示す図

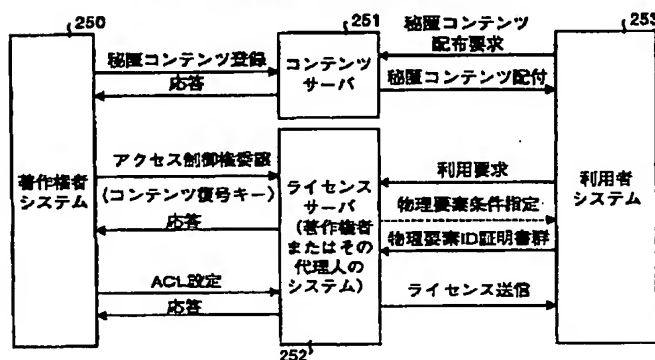


【図19】

改良したアクセス制御モデルを示す図

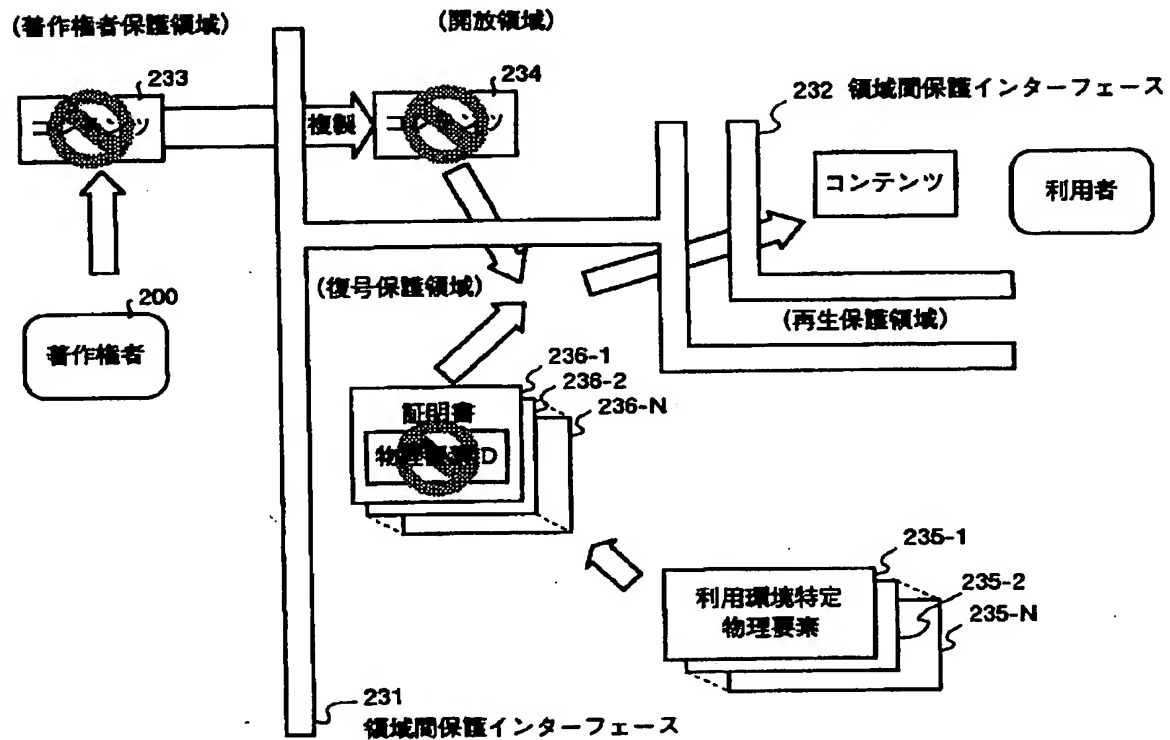


【図22】

図21に示したコンテンツキャッシュ可能型モデルに対応する
コンテンツ利用制御システムの概要構成を示す図

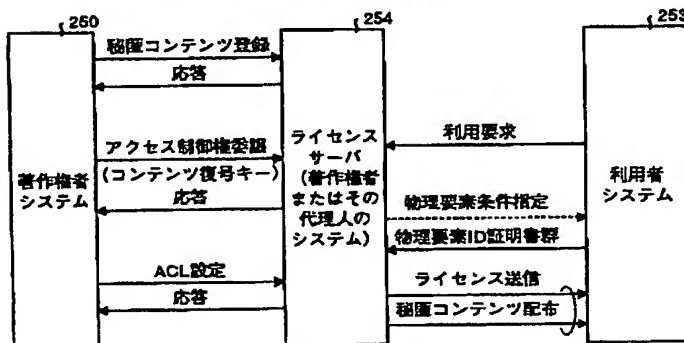
【図20】

従来のコンテンツ利用制御システムのコンテンツ配布モデルを示す図



【図23】

コンテンツ同時配布型モデルを実現するコンテンツ利用制御システムの概要構成を示す図



コンテンツキャッシュ可能型モデルを示す図

The diagram illustrates a content caching model with the following components and flow:

- Copyright Protection Domain (著作権保護領域):** Contains the **Content Creator (著作権者 200)** and a **Copyright Key (Kc)**. The creator provides **Content (コンテンツ 243-1, 243-2, ..., 243-N)** and a **Physical Element ID (物理要素ID 243-1, 243-2, ..., 243-N)** to the user.
- User (利用者 205):** Receives the content and physical element IDs. The user also has their own **Content (コンテンツ 244)**.
- Open Domain (開放領域):** A central area where content is distributed. It includes a **Cache (キャッシュ 234)** and a **License (ライセンス)** key.
- Secret Key Protection Domain (秘密保護領域):** Contains a **Secret Key (Kp)** and a **Physical Element ID (物理要素ID 243-1, 243-2, ..., 243-N)**. This domain is used for secure distribution and verification.
- Physical Element ID (物理要素ID):** A series of IDs (243-1, 243-2, ..., 243-N) that link the content to the physical elements and the secret key.
- License (ライセンス):** A key used for content verification and distribution.
- Cache (キャッシュ 234):** A storage unit for content and physical element IDs.
- Physical Element ID (物理要素ID):** A series of IDs (243-1, 243-2, ..., 243-N) that link the content to the physical elements and the secret key.
- Secret Key (Kp):** A key used for secure distribution and verification.
- Physical Element ID (物理要素ID):** A series of IDs (243-1, 243-2, ..., 243-N) that link the content to the physical elements and the secret key.
- Physical Element ID (物理要素ID):** A series of IDs (243-1, 243-2, ..., 243-N) that link the content to the physical elements and the secret key.

F ターム(参考) 5B017 AA01 AA07 BA05 BA07 BB03
BB10 CA07 CA08 CA09 CA12
CA14 CA15 CA16
5B085 AC03 AE06 AE29